Source and Channel Polarization over Finite Fields and Reed-Solomon Matrix

Ryuhei Mori *Student Member, IEEE* and Toshiyuki Tanaka *Member, IEEE*

Abstract

Polarization phenomenon over any finite field $\mathbb{F}_q$ with size q being a power of a prime is considered. This problem is a generalization of the original proposal of channel polarization by Arıkan for the binary field, as well as its extension to a prime field by Şaşoğlu, Telatar, and Arıkan. In this paper, a necessary and sufficient condition of a matrix over a finite field $\mathbb{F}_q$ is shown under which any source and channel are polarized. Furthermore, the result of the speed of polarization for the binary alphabet obtained by Arıkan and Telatar is generalized to arbitrary finite field. It is also shown that the asymptotic error probability of polar codes is improved by using the Reed-Solomon matrix, which can be regarded as a natural generalization of the 2×2 binary matrix used in the original proposal by Arıkan.

Index Terms

Polar code, channel polarization, source polarization, Reed-Solomon code, Reed-Muller code.

I. Introduction

ARIKAN introduced the method of channel and source polarization which gives an efficient capacity-achieving binary source and channel codes, respectively [3]. Şaşoğlu et al. generalized the polarization phenomenon to non-binary alphabets whose size is a prime [4]. In this paper, we further extend the polarization phenomenon to non-binary alphabets whose size is a power of a prime by using finite fields.

The contributions of this paper are threefold. The first contribution is that we give a complete characterization as to whether an $\ell \times \ell$ matrix over a finite field gives rise to polarization. This extends the result on the binary field by Korada et al. [5] to a general finite field. The second contribution is that we characterize the asymptotic speed of polarization in terms of the matrix used. This is again an extension of the result on the binary field by Korada et al. [5] to a general finite field. The third contribution of this paper is that we provide an explicit construction of an $\ell \times \ell$ matrix, which is based on the Reed-Solomon matrix, with asymptotically the fastest polarization for $\ell \leq q$.

The organization of this paper is as follows. In Section II, notations and definitions used in this paper are introduced. In Section III, the basic transform of a source and polarization phenomenon by an $\ell \times \ell$ matrix over a finite field are introduced. In Section IV, an equivalence relation of q-ary source is defined for showing equivalence among several polarization problems. On the concept of equivalence among sources, equivalence of matrices is considered as well. Using the equivalence of matrices, the main theorem of this paper is stated here, which is a necessary and sufficient condition of matrix under which any source or channel is polarized. In Section V, the Bhattacharyya parameter and its properties are shown. They are useful for proving the main theorem in Section VI and speed of the polarization in Section VII. In Section VI, a proof of the main theorem is shown. In Section VII, the speed of the polarization for a general $\ell \times \ell$ matrix is proved similarly to the binary case. In Section VIII, the Reed-Solomon matrix is introduced, which yields asymptotically fast polarization in the sense discussed in Section VII. In Section IX, the quaternary polar codes using the Reed-Solomon matrix is compared numerically with the original binary polar codes. Finally, Section X summarizes the paper.

II. Preliminaries

Let p be a prime number and $q := p^m$ where m is a natural number. Let $\mathbb{F}_q$ be a finite field of size q. Let $\mathbb{F}_q^\times$ be $\mathbb{F}_q \setminus \{0\}$ and $\mathbb{F}_p(\gamma)$ be the simple extension of $\mathbb{F}_p$ generated by the adjunction of $\gamma \in \mathbb{F}_q$. Similarly, for $A \subseteq \mathbb{F}_q$ and a matrix G over $\mathbb{F}_q$, $\mathbb{F}_p(A)$ and $\mathbb{F}_p(G)$ denote the field extension of $\mathbb{F}_p$ generated by the adjunction of all elements of A and G, respectively. Let $\Delta_q := \{[p_1, \dots, p_q] \in \mathbb{R}_{\geq 0}^q \mid p_1 + \cdots + p_q = 1\}$ denote the set of all q-dimensional probability vectors. For random variables X on a finite set $\mathcal{X}$ of size q and Y on a discrete set $\mathcal{Y}$, entropy $H(X)$ of X and conditional entropy $H(X \mid Y)$ of X conditioned on Y are defined as

$$H(X) := -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x)$$
$$H(X \mid Y) := -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} P_{X,Y}(x, y) \log P_{X|Y}(x \mid y).$$

This paper was presented in part at [1], [2]. The work of R. Mori was supported by the Grant-in-Aid for Scientific Research for JSPS Fellows (22·5936). The work of T. Tanaka was supported by the Grant-in-Aid for Scientific Research (C), JSPS, Japan (22560375).

R. Mori and T. Tanaka are with the Department of Systems Science, Graduate School of Informatics, Kyoto University, Yoshida Hon-machi, Sakyo-ku, Kyoto-shi, Kyoto, 606-8501 Japan (e-mail: rmori@sys.i.kyoto-u.ac.jp, tt@i.kyoto-u.ac.jp).

In this paper, the base of the logarithm is assumed to be q unless otherwise stated, and hence $H(X)$ and $H(X \mid Y)$ are in $[0,1]$. If a quantity $A((X,Y))$ determined from $P_{X,Y}$ has the form $\mathbb{E}[f([P_{X|Y}(x \mid Y)]_{x\in\mathbb{F}_q})]$ for some $f : \Delta_q \to \mathbb{R}$, where $\mathbb{E}$ denotes the expectation, we write it as $A(X \mid Y)$. It should be noted that the arguments in this paper are directly applicable to the case where $\mathcal{Y}$ is a continuous alphabet such as $\mathbb{R}$, by replacing the summation $\sum_{y\in\mathcal{Y}}$ with the integral $\int_{-\infty}^{+\infty} \mathrm{d}y$. The notation $u_0^{\ell-1}$ denotes the row vector $[u_0, u_1, \dots, u_{\ell-1}]$.

III. Source and channel polarization

A. Source and channel polarization phenomenon

In this paper, we consider source polarization on an $\ell \times \ell$ invertible matrix G over $\mathbb{F}_q$. Let a q-ary source (X,Y) be defined as a pair of random variables on $\mathbb{F}_q \times \mathcal{Y}$. We first introduce a basic transform of source, $(X,Y) \to \{(X^{(i)}, Y^{(i)})\}_{i=0,\dots,\ell-1}$. Let $\{(X_i, Y_i)\}_{i=0,\dots,\ell-1}$ be ℓ independent drawings of (X,Y). Let $U_0^{\ell-1}$ be a random vector defined by the equation $X_0^{\ell-1} = U_0^{\ell-1}G$. Letting $(X^{(i)}, Y^{(i)}) := (U_i, (U_0^{i-1}, Y_0^{\ell-1}))$ for $i = 0, \dots, \ell-1$ defines the basic transform $(X,Y) \to \{(X^{(i)}, Y^{(i)})\}_{i=0,\dots,\ell-1}$ where the random pair $(X^{(i)}, Y^{(i)})$ takes values in $\mathbb{F}_q \times (\mathbb{F}_q^i \times \mathcal{Y}^\ell)$. From the chain rule for the entropy, one has

$$\ell H(X \mid Y) = H(X_0^{\ell-1} \mid Y_0^{\ell-1}) = H(U_0^{\ell-1} \mid Y_0^{\ell-1}) = \sum_{i=0}^{\ell-1} H(U_i \mid U_0^{i-1}, Y_0^{\ell-1}) = \sum_{i=0}^{\ell-1} H(X^{(i)} \mid Y^{(i)}). \tag{1}$$

By starting with a source (X,Y) and recursively applying the basic transform to depth n, we obtain ℓ^n random pairs $\{(X^{(b_1)\cdots(b_n)}, Y^{(b_1)\cdots(b_n)})\}_{(b_1,\dots,b_n)\in\{0,\dots,\ell-1\}^n}$[1]. Let $B_1, \dots, B_n, \dots$ be independent uniform random variables on $\{0,\dots,\ell-1\}$. Let $(\mathsf{X}_n, \mathsf{Y}_n) := (X^{(B_1)\cdots(B_n)}, Y^{(B_1)\cdots(B_n)})$ for $n \in \{0,1,\dots\}$. A random sequence $\{H_n : \sigma(B_1,\dots,B_n)\text{-measurable}\}_{n=0,1,\dots}$ is defined as $H_n := H(\mathsf{X}_n \mid \mathsf{Y}_n)$ where the conditional entropy does not take account of randomness of $(B_1,\dots,B_n)$. From the chain rule (1) for the entropy, the random sequence $\{H_n\}_{n=0,1,\dots}$ is shown to be a martingale i.e., $\mathbb{E}[H_n \mid B_1,\dots,B_{n-1}] = H_{n-1}$. Then, noting that the sequence $\{H_n\}_{n=0,1,\dots}$ is bounded in the interval $[0,1]$, from the martingale convergence theorem, there exists a random variable H_∞ such that H_n converges to H_∞ almost surely. The source polarization is defined in terms of H_∞ as in the following definition.

Definition 1 (Polarization)**.** A source (X,Y) is said to be polarized by G if and only if

$$H_\infty = \begin{cases} 0, & \text{with probability } 1 - H(X \mid Y) \\ 1, & \text{with probability } H(X \mid Y). \end{cases} \tag{2}$$

It should be noted that if H_∞ is $\{0,1\}$-valued, the probability of $H_\infty = 1$ is necessarily equal to $H(X \mid Y)$ because of the martingale property $\mathbb{E}[H_n \mid H_0] = H_0 = H(X \mid Y)$.

When the marginal distribution of X is uniform, the source polarization is called the channel polarization. As shown in Section IV, the source polarization problem is also translated into the channel polarization problem. We therefore use the terms “source” and “channel” almost interchangeably, unless otherwise stated. As the first and main contribution of this paper, we show a necessary and sufficient condition of G under which any source or channel is polarized. Let $G_\gamma := \begin{bmatrix} 1 & 0 \\ 1 & \gamma \end{bmatrix}$ over $\mathbb{F}_q$ where $\gamma \in \mathbb{F}_q^\times$. Arıkan proved for the case $q = 2$ that the matrix G_1 polarizes any source/channel [3], [6]. Şaşoğlu et al. generalized the result for prime fields [4]. They also showed that for the matrix G_1 over the ring $\mathbb{Z}/q\mathbb{Z}$ where q is not a prime, there is a counterexample of non-polarizing q-ary channel. Their counterexample also works for $\mathbb{F}_q$ whose size q is not a prime. Our purpose of this paper is to generalize these results to any matrix over any finite field.

B. Construction of source and channel codes

The polar code for source/channel coding is based on the polarization phenomenon. In this subsection, a rough sketch of construction of the polar code for channel coding is described. Given an $\ell \times \ell$ invertible matrix G which appears in the previous section, we first consider an $\ell^n \times \ell^n$ matrix $G^{\otimes n}$ where ${}^{\otimes n}$ denotes the Kronecker power. For $i \in \{0,1,\dots,\ell^n - 1\}$, $i_n i_{n-1} \cdots i_1$ denotes the ℓ-ary expansion of i. Then, the generator matrix of a polar code is, roughly speaking, obtained from $G^{\otimes n}$ by choosing rows with indices[2] in the set

$$\{i \in \{0,\dots,\ell^n - 1\} \mid H(X^{(i_1)\cdots(i_n)} \mid Y^{(i_1)\cdots(i_n)}) < \epsilon\}$$

with some threshold $\epsilon > 0$. If a channel (X,Y) is polarized by G, the ratio of chosen rows is asymptotically $1 - H(X \mid Y)$ for any fixed $\epsilon \in (0,1)$. For detailed descriptions of encoding and decoding algorithms, see [3] for the channel coding and [6] and [7] for the source coding.

[1] Joint distribution of these random pairs is not considered in this paper.

[2] Row and column indices of matrices start with 0 rather than 1.

IV. Equivalence relation on sources and main theorem

In order to deal with a source (X,Y) in terms of polarization phenomenon, it is useful to define an equivalence relation up to which we do not have to distinguish sources. An equivalence relation $(X,Y)\sim(X',Y')$ which is desirable for our purpose has to satisfy the following two conditions.

$$(X,Y)\sim(X',Y')\Longrightarrow H(X\mid Y)=H(X'\mid Y') \tag{3}$$

$$(X,Y)\sim(X',Y')\Longrightarrow (X^{(i)},Y^{(i)})\sim(X'^{(i)},Y'^{(i)}) \text{ for } i=0,1,\dots,\ell-1 \tag{4}$$

The second condition (4) should be satisfied for any $\ell\times\ell$ invertible matrix G. The significance of these two conditions is that sources which are equivalent in the above sense yield the same random sequence $\{H_n\}_{n=0,1,\dots}$, thereby behaving exactly the same as for the polarization phenomenon.

Given a source (X,Y), the a posteriori distribution $[p_{X|Y}(x\mid y)]_{x\in\mathbb{F}_q}\in\Delta_q$ plays a fundamental role, in particular in determining the conditional entropy $H(X\mid Y)$ and other relevant quantities. We first introduce two equivalence relations on probability vectors.

Definition 2. For $p_0^{q-1}\in\Delta_q$ and $p'^{q-1}_0\in\Delta_q$, we say $p_0^{q-1}\overset{\mathrm{p}}{\sim}p'^{q-1}_0$ if and only if there exists a permutation matrix σ such that $p_0^{q-1}=p'^{q-1}_0\sigma$. For any $s\in\mathbb{N}$, $[p_{\boldsymbol{x}}]_{\boldsymbol{x}\in\mathbb{F}_q^s}\in\Delta_{q^s}$ and $[p'_{\boldsymbol{x}}]_{\boldsymbol{x}\in\mathbb{F}_q^s}\in\Delta_{q^s}$, we say $[p_{\boldsymbol{x}}]_{\boldsymbol{x}\in\mathbb{F}_q^s}\overset{\mathrm{q}}{\sim}[p'_{\boldsymbol{x}}]_{\boldsymbol{x}\in\mathbb{F}_q^s}$ if and only if there exists $\boldsymbol{z}\in\mathbb{F}_q^s$ such that $p_{\boldsymbol{x}}=p'_{\boldsymbol{x}+\boldsymbol{z}}$ for all $\boldsymbol{x}\in\mathbb{F}_q^s$.

It is straightforward to see that

$$[p_{\boldsymbol{x}}]_{\boldsymbol{x}\in\mathbb{F}_q^s}\overset{\mathrm{q}}{\sim}[p'_{\boldsymbol{x}}]_{\boldsymbol{x}\in\mathbb{F}_q^s}\iff[p_{\boldsymbol{x}H}]_{\boldsymbol{x}\in\mathbb{F}_q^s}\overset{\mathrm{q}}{\sim}[p'_{\boldsymbol{x}H}]_{\boldsymbol{x}\in\mathbb{F}_q^s} \tag{5}$$

holds for any $s\times s$ invertible matrix H since $p_{\boldsymbol{x}}=p'_{\boldsymbol{x}+\boldsymbol{z}}\iff p_{\boldsymbol{x}H}=p'_{\boldsymbol{x}H+\boldsymbol{z}H}$ for any $\boldsymbol{z}\in\mathbb{F}_q^s$.

The q-dimensional random vector $[p_{X|Y}(x\mid Y)]_{x\in\mathbb{F}_q}\in\Delta_q$ induces a probability measure on Δ_q. If two random vectors $[p_{X|Y}(x\mid Y)]_{x\in\mathbb{F}_q}$ and $[p_{X'|Y'}(x\mid Y')]_{x\in\mathbb{F}_q}$ defined from sources (X,Y) on $\mathbb{F}_q\times\mathcal{Y}$ and (X',Y') on $\mathbb{F}_q\times\mathcal{Y}'$, respectively, induce the same probability measure on Δ_q, we say $(X,Y)\overset{\mathrm{i}}{\sim}(X',Y')$. In this case, $A(X\mid Y)=A(X'\mid Y')$ holds for any quantity of the form $A(X\mid Y)=\mathbb{E}[f([p_{X|Y}(x\mid Y)]_{x\in\mathbb{F}_q})]$, and hence the condition (3) is satisfied. Furthermore, the equivalence relation $\overset{\mathrm{i}}{\sim}$ obviously satisfies (4). However, a weaker equivalence relation than $\overset{\mathrm{i}}{\sim}$ exists which satisfies both of the conditions (3) and (4). First, a weak equivalence relation which only satisfies the condition (3) is defined as follows.

Definition 3. For sources (X,Y) on $\mathbb{F}_q\times\mathcal{Y}$ and (X',Y') on $\mathbb{F}_q\times\mathcal{Y}'$, we say $(X,Y)\overset{\mathrm{s}}{\sim}(X',Y')$ if and only if the q-dimensional random vector $[P_{X|Y}(x\mid Y)]_{x\in\mathbb{F}_q}$ induces the same distribution on $\Delta_q/\overset{\mathrm{p}}{\sim}$ as the random vector $[P_{X'|Y'}(x\mid Y')]_{x\in\mathbb{F}_q}$. For a function $f:\Delta_q\to\mathbb{R}$ which is invariant under any permutation of its arguments, a quantity $\mathbb{E}[f([P_{X|Y}(x\mid Y)]_{x\in\mathbb{F}_q})]$ is said to be invariant under any permutation of symbols in a posteriori distribution.

The equivalence $(X,Y)\overset{\mathrm{s}}{\sim}(X',Y')$ implies $A(X\mid Y)=A(X'\mid Y')$ for any quantity $A(X\mid Y)$ invariant under any permutation of symbols in a posteriori distribution, including the conditional entropy $H(X\mid Y)$. Hence, the equivalence relation $\overset{\mathrm{s}}{\sim}$ satisfies the first condition (3). However, the equivalence relation $\overset{\mathrm{s}}{\sim}$ does not satisfy the second condition (4). The equivalence relation $\overset{\mathrm{a}}{\sim}$ defined in the following is weaker than $\overset{\mathrm{i}}{\sim}$ and satisfies both of the conditions (3) and (4).

Definition 4. Let $s\in\mathbb{N}$. For pairs of random variables (X,Y) on $\mathbb{F}_q^s\times\mathcal{Y}$ and (X',Y') on $\mathbb{F}_q^s\times\mathcal{Y}'$, we say $(X,Y)\overset{\mathrm{a}}{\sim}(X',Y')$ if and only if there exists $r\in\mathbb{F}_q^\times$ such that the q^s-dimensional random vector $[P_{X|Y}(r\boldsymbol{x}\mid Y)]_{\boldsymbol{x}\in\mathbb{F}_q^s}$ induces the same distribution on $\Delta_{q^s}/\overset{\mathrm{q}}{\sim}$ as $[P_{X'|Y'}(\boldsymbol{x}\mid Y')]_{\boldsymbol{x}\in\mathbb{F}_q^s}$.

It is not hard to confirm the properties $(X,Y)\overset{\mathrm{i}}{\sim}(X',Y')\Longrightarrow(X,Y)\overset{\mathrm{a}}{\sim}(X',Y')$ and $(X,Y)\overset{\mathrm{a}}{\sim}(X',Y')\Longrightarrow(X,Y)\overset{\mathrm{s}}{\sim}(X',Y')$. From the latter property, it holds that $(X,Y)\overset{\mathrm{a}}{\sim}(X',Y')\Longrightarrow H(X\mid Y)=H(X'\mid Y')$, implying that the equivalence relation $\overset{\mathrm{a}}{\sim}$ satisfies the first condition (3). The equivalence relation $\overset{\mathrm{a}}{\sim}$ also satisfies the second condition (4).

Lemma 5.

$$(X,Y)\overset{\mathrm{a}}{\sim}(X',Y')\Longrightarrow(X^{(i)},Y^{(i)})\overset{\mathrm{a}}{\sim}(X'^{(i)},Y'^{(i)})\ \textit{for}\ i=0,1,\dots,\ell-1$$

for an arbitrary $\ell\times\ell$ invertible matrix G.

Proof: For a source (X,Y), let $X_0^{\ell-1}$, $Y_0^{\ell-1}$ and $U_0^{\ell-1}$ be what appear in the definition of the basic transform of it. The random variables $X'^{\ell-1}_0$, $Y'^{\ell-1}_0$ and $U'^{\ell-1}_0$ are defined in the same way for (X',Y'). The equivalence relation $(X,Y)\overset{\mathrm{a}}{\sim}(X',Y')$ between sources (X,Y) and (X',Y') immediately leads to the equivalence $(X_0^{\ell-1},Y_0^{\ell-1})\overset{\mathrm{a}}{\sim}(X'^{\ell-1}_0,Y'^{\ell-1}_0)$ between their ℓth-order extensions. From (5) and the identity $(r\boldsymbol{x})G^{-1}=r(\boldsymbol{x}G^{-1})$ for any $r\in\mathbb{F}_q^\times$ and $\boldsymbol{x}\in\mathbb{F}_q^\ell$, it holds that $(X_0^{\ell-1}G^{-1},Y_0^{\ell-1})\overset{\mathrm{a}}{\sim}(X'^{\ell-1}_0G^{-1},Y'^{\ell-1}_0)$, or equivalently, $(U_0^{\ell-1},Y_0^{\ell-1})\overset{\mathrm{a}}{\sim}(U'^{\ell-1}_0,Y'^{\ell-1}_0)$. One therefore obtains $(U_i,(U_0^{i-1},Y_0^{\ell-1}))\overset{\mathrm{a}}{\sim}(U'_i,(U'^{i-1}_0,Y'^{\ell-1}_0))$. ■

The equivalence relation $\overset{\mathrm{a}}{\sim}$ gives rise to the following several useful lemmas.

Lemma 6 (Source-channel equivalence [8]). *Let (N, Z) be a random pair on $\mathbb{F}_q \times \mathcal{Y}$ and X be a uniform random variable on $\mathbb{F}_q$ which is independent of (N, Z). Then, it holds that $(N, Z) \overset{\mathrm{a}}{\sim} (X, (X + N, Z))$.*

Proof: One has $(X, (X+N, Z)) \overset{\mathrm{a}}{\sim} (-X+(X+N), (X+N, Z)) = (N, (X+N, Z)) \overset{\mathrm{i}}{\sim} (N, Z)$, where the last equivalence relation is due to the assumptions on X. ■

The channel $(X, (X + N, Z))$ in Lemma 6 is a symmetric channel in the following sense.

Definition 7 (Symmetric channel). A channel (X, Y) on $\mathbb{F}_q \times \mathcal{Y}$ is said to be symmetric if and only if there exists a permutation σ_x on $\mathcal{Y}$ for each $x \in \mathbb{F}_q$ such that $P_{Y|X}(y \mid x) = P_{Y|X}(\sigma_{x'-x}(y) \mid x')$ for any $y \in \mathcal{Y}$ and $x, x' \in \mathbb{F}_q$.

The symmetricity is preserved under the basic transform.

Lemma 8. *For a symmetric channel (X, Y), $(X^{(i)}, Y^{(i)})$ is symmetric for any $i \in \{0, \dots, \ell - 1\}$.*

Proof: The statement holds since $P_{U_0^{\ell-1}, Y_0^{\ell-1}}((u_0^{i-1}, u_i, u_{i+1}^{\ell-1}), y_0^{\ell-1}) = P_{U_0^{\ell-1}, Y_0^{\ell-1}}((u_0^{i-1}, u_i', u_{i+1}^{\ell-1}), w_0^{\ell-1})$ where $w_j = \sigma_{G_{i,j}(u_i'-u_i)}(y_j)$. ■

Lemma 9. *For any channel (X, Y) and any symmetric channel (X', Y'), let $(Z, (Y, Y'))$ and $(Z', (Y, Y'))$ be the channels defined by letting $Z = X = X'$ and $Z' = X = X' + a$ for any fixed $a \in \mathbb{F}_q$, respectively. For these channels, it holds that $(Z, (Y, Y')) \overset{\mathrm{i}}{\sim} (Z', (Y, Y'))$.*

Proof: The equality $P_{Z,(Y,Y')}(z, (y, y')) = P_{Z',(Y,Y')}(z, (y, \sigma_a^{-1}(y')))$ implies $(Z, (Y, Y')) \overset{\mathrm{i}}{\sim} (Z', (Y, Y'))$. ■

We say that $\ell \times \ell$ invertible matrices $\hat{G}$ and $\bar{G}$ are equivalent when $(\hat{X}^{(i)}, \hat{Y}^{(i)}) \overset{\mathrm{a}}{\sim} (\bar{X}^{(i)}, \bar{Y}^{(i)})$ for $i = 0, \dots, \ell - 1$ where $\{(\hat{X}^{(i)}, \hat{Y}^{(i)})\}_{i=0,\dots,\ell-1}$ and $\{(\bar{X}^{(i)}, \bar{Y}^{(i)})\}_{i=0,\dots,\ell-1}$ are two sets of ℓ random pairs generated from an arbitrary common source (X, Y) via the basic transform using matrices $\hat{G}$ and $\bar{G}$, respectively.

Lemma 10. *Let G and V be an $\ell \times \ell$ invertible matrix and an $\ell \times \ell$ invertible upper triangular matrix, respectively. Then, G and VG are equivalent.*

Proof: Since $X_0^{\ell-1} = U_0^{\ell-1} VG \iff X_0^{\ell-1} G^{-1} = U_0^{\ell-1} V =: U'^{\ell-1}_0$, the equivalence $(U_i, (U_0^{i-1}, Y_0^{\ell-1})) \overset{\mathrm{a}}{\sim} (U_i', (U'^{i-1}_0, Y_0^{\ell-1}))$ implies the lemma. ■

Obviously, a permutation of columns of G does not change $(X^{(i)}, Y^{(i)})$ up to the equivalence $\overset{\mathrm{i}}{\sim}$ for $i = 0, \dots, \ell - 1$, so that G and its column permutation are equivalent. Hence, without loss of generality, one can assume that G is a lower triangular matrix. Lower triangular matrices with unit diagonal elements equivalent to G are called standard forms of G. A standard form of G is not generally unique. Note that the standard forms of G_γ are $\begin{bmatrix} 1 & 0 \\ \gamma^{-1} & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix}$. If there exists the identity matrix as a standard form of G, it is the unique standard form of G. In this case, one obviously has the identity $(X^{(i)}, Y^{(i)}) \overset{\mathrm{a}}{\sim} (X, Y)$ for all $i \in \{0, \dots, \ell - 1\}$, implying that G does not polarize any source. For other cases, the following main theorem shows necessary and sufficient conditions of G under which any source is polarized.

Theorem 11. *The followings are equivalent for an $\ell \times \ell$ invertible matrix G over $\mathbb{F}_q$ with a non-identity standard form.*

- *Any q-ary source is polarized by G.*
- *It holds $\mathbb{F}_p(\bar{G}) = \mathbb{F}_q$ for any standard form $\bar{G}$ of G.*
- *It holds $\mathbb{F}_p(\bar{G}) = \mathbb{F}_q$ for one of the standard form $\bar{G}$ of G.*

Corollary 12. *Any q-ary source is polarized by the 2×2 matrix G_γ over $\mathbb{F}_q$ with $\gamma \in \mathbb{F}_q^\times$ if and only if $\mathbb{F}_p(\gamma) = \mathbb{F}_q$.*

Note that the identity matrix is the standard form of an invertible matrix G if and only if there exists an upper triangular matrix as a column permutation of G. Thus, Theorem 11 includes the known results that an invertible matrix G is polarizing if and only if any column permutation of G is not upper triangular for $q = 2$ [5, Lemma 1] and for q prime [4].

V. Bhattacharyya parameter

Bhattacharyya parameter is useful both for proving the polarization phenomenon, and for evaluating asymptotic speed of polarization. In this section, it is shown that polarization of Bhattacharyya parameter and polarization of the conditional entropy are equivalent. Let $(\Omega := \{1, \dots, q\}, 2^\Omega, P)$ be a probability space. The probability measure P can be represented by the vector $[\sqrt{P(1)}, \dots, \sqrt{P(q)}] \in \mathcal{S}_q$ where $\mathcal{S}_q := \{[p_1, \dots, p_q] \in \mathbb{R}^q_{\geq 0} \mid p_1^2 + \cdots + p_q^2 = 1\}$. The L_p norm of $\boldsymbol{x} \in \mathbb{C}^q$ is defined as $L_p(\boldsymbol{x}) := (|x_1|^p + \cdots + |x_q|^p)^{1/p}$ for any $p \geq 1$. The L_1 norm of $\boldsymbol{p} \in \mathcal{S}_q$ attains the minimum 1 at the deterministic distributions i.e., the distributions of the form $[0, \dots, 0, 1, 0, \dots, 0]$, and the maximum $\sqrt{q}$ at the uniform distribution, represented by $\boldsymbol{u} := [1/\sqrt{q}, \dots, 1/\sqrt{q}] \in \mathcal{S}_q$. On the other hand, the deterministic and uniform distributions also minimize and maximize the entropy $H(\boldsymbol{p}) := -\sum_i p_i^2 \log p_i^2$ of $\boldsymbol{p} \in \mathcal{S}_q$, respectively.

The following lemma states that closeness of a probability distribution to determinism or uniformity measured in terms of its entropy value is equivalent to that measured in terms of its L_1-norm value.

Lemma 13. *For any* $\epsilon > 0$, *there exists* $\delta > 0$ *such that*

$$\{\boldsymbol{p} \in \mathcal{S}_q \mid H(\boldsymbol{p}) < \delta\} \subseteq \{\boldsymbol{p} \in \mathcal{S}_q \mid L_1(\boldsymbol{p}) - 1 < \epsilon\} \tag{6}$$

$$\{\boldsymbol{p} \in \mathcal{S}_q \mid L_1(\boldsymbol{p}) - 1 < \delta\} \subseteq \{\boldsymbol{p} \in \mathcal{S}_q \mid H(\boldsymbol{p}) < \epsilon\} \tag{7}$$

$$\{\boldsymbol{p} \in \mathcal{S}_q \mid 1 - H(\boldsymbol{p}) < \delta\} \subseteq \{\boldsymbol{p} \in \mathcal{S}_q \mid \sqrt{q} - L_1(\boldsymbol{p}) < \epsilon\} \tag{8}$$

$$\{\boldsymbol{p} \in \mathcal{S}_q \mid \sqrt{q} - L_1(\boldsymbol{p}) < \delta\} \subseteq \{\boldsymbol{p} \in \mathcal{S}_q \mid 1 - H(\boldsymbol{p}) < \epsilon\}. \tag{9}$$

Proof: Since

$$L_2(\boldsymbol{u} - \boldsymbol{p})^2 = \sum_{i=1}^{q} \left(\frac{1}{\sqrt{q}} - p_i\right)^2 = 2 - \frac{2}{\sqrt{q}} \sum_{i=1}^{q} p_i = \frac{2}{\sqrt{q}} \left(\sqrt{q} - L_1(\boldsymbol{p})\right)$$

(9) is a consequence of continuity of $H(\boldsymbol{p})$. The relationship (8) follows from

$$1 - H(\boldsymbol{p}) = 1 + \sum_{i=1}^{q} p_i^2 \log p_i^2 = -2 \sum_{i=1}^{q} p_i^2 \log \frac{1}{\sqrt{q} p_i} \ge \frac{2}{\log_{\mathrm{e}} q} \sum_{i=1}^{q} p_i^2 \left(1 - \frac{1}{\sqrt{q} p_i}\right) = \frac{2}{\sqrt{q} \log_{\mathrm{e}} q} \left(\sqrt{q} - L_1(\boldsymbol{p})\right).$$

Since $H(\boldsymbol{p}) = 2\sum_i p_i^2 \log(1/p_i) \le 2 \log \sum_i p_i = 2 \log L_1(\boldsymbol{p})$, the relationship (7) holds. Since $H(\boldsymbol{p}) \log_{\mathrm{e}} q = -\sum_i p_i^2 \log_{\mathrm{e}} p_i^2 \ge -\log_{\mathrm{e}} \max_i p_i^2 \ge 1 - \max_i p_i^2 \ge (L_1(\boldsymbol{p}) - 1)^2/(q-1)$ (see (22) for the last inequality), the relationship (6) holds. ■

Hence, the entropy is close to 0 and 1 if and only if the L_1 norm is close to 1 and $\sqrt{q}$, respectively. From Lemma 13 and the following observation of inequalities about expectation of the square of L_1 norm,

$$1 \le \sum_{y \in \mathcal{Y}} P_Y(y) \left[\sum_{x \in \mathbb{F}_q} \sqrt{P_{X|Y}(x \mid y)}\right]^2 \le q$$

$$\iff 0 \le \frac{1}{q-1} \sum_{\substack{x \in \mathbb{F}_q, x' \in \mathbb{F}_q \\ x \ne x'}} \sum_{y \in \mathcal{Y}} P_Y(y) \sqrt{P_{X|Y}(x \mid y) P_{X|Y}(x' \mid y)} \le 1$$

for a random pair (X, Y), the conditional entropy $H(X \mid Y)$ is close to 0 and 1 if and only if the Bhattacharyya parameter $Z(X \mid Y) \in [0, 1]$ for (X, Y), defined as

$$Z(X \mid Y) := \frac{1}{q-1} \sum_{\substack{x \in \mathbb{F}_q, x' \in \mathbb{F}_q \\ x \ne x'}} \sum_{y \in \mathcal{Y}} P_Y(y) \sqrt{P_{X|Y}(x \mid y) P_{X|Y}(x' \mid y)}$$

is close to 0 and 1, respectively. Obviously, $Z(X \mid Y)$ is invariant under any permutation of symbols in a posteriori distribution of (X, Y). For $d \in \mathbb{F}_q^\times$, we define $Z_d(X \mid Y) \in [0, 1]$ as

$$Z_d(X \mid Y) := \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathcal{Y}} P_Y(y) \sqrt{P_{X|Y}(x \mid y) P_{X|Y}(x + d \mid y)}.$$

The Bhattacharyya parameter $Z(X \mid Y)$ can be expressed as the average of $Z_d(X \mid Y)$

$$Z(X \mid Y) = \frac{1}{q-1} \sum_{d \in \mathbb{F}_q^\times} Z_d(X \mid Y).$$

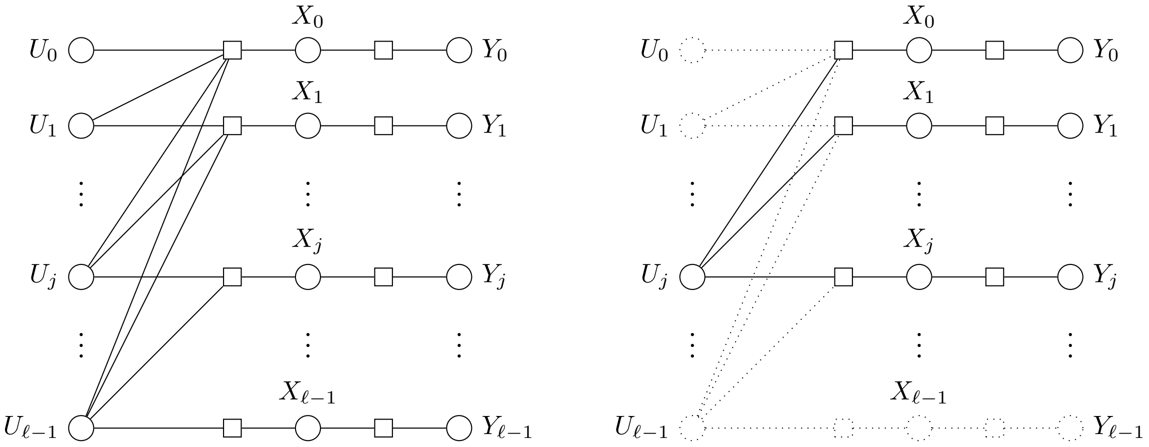
Hence, $Z(X \mid Y)$ is close to 0 and 1 if and only if $Z_d(X \mid Y)$ is simultaneously close to 0 and 1 for all $d \in \mathbb{F}_q^\times$, respectively.

Note that the Rényi entropy, which is similar to the L_p norm, also explains the Bhattacharyya parameter.

VI. Proof of the Main Theorem

A. Sketch

In this section, the proof of Theorem 11 is shown. In Section VI-B, it is proved that if there exists a standard form $\bar{G}$ of G such that $\mathbb{F}_p(\bar{G}) \ne \mathbb{F}_q$, there exists a source which is not polarized by G. It means that if any source is polarized by G, any standard form $\bar{G}$ of G satisfies $\mathbb{F}_p(\bar{G}) = \mathbb{F}_q$. In Section VI-C, it is proved that if there exists a standard form $\bar{G}$ of G such that $\mathbb{F}_p(\bar{G}) = \mathbb{F}_q$, any source is polarized by G. This completes the proof of Theorem 11.



(a) Complete representation.

(b) Representation under conditioning.

Fig. 1. Tanner-graph representations of the relationship among $U_0^{\ell-1}$, $X_0^{\ell-1}$ and $Y_0^{\ell-1}$ with a standard form $\bar{G}$.

B. Necessity

Let $\bar{G}$ be an arbitrary standard form of G. Assume $\mathbb{F}_p(\bar{G}) \neq \mathbb{F}_q$. Let $M := [\mathbb{F}_q : \mathbb{F}_p(\bar{G})]$ be a degree of a field extension $\mathbb{F}_q/\mathbb{F}_p(\bar{G})$. Fix a basis of a linear space $\mathbb{F}_q/\mathbb{F}_p(\bar{G})$. Each $x \in \mathbb{F}_q$ is naturally identified with an M-dimensional vector over $\mathbb{F}_p(\bar{G})$ according to the fixed basis. Let $[V_0, \dots, V_{M-1}] \in \mathbb{F}_p(\bar{G})^M$ be a random vector corresponding to $X \in \mathbb{F}_q$ according to the identification between $\mathbb{F}_p(\bar{G})^M$ and $\mathbb{F}_q$. If one takes a source (X, Y) for which $V_0, \dots, V_{M-1}$ are independent conditioned on Y, recursive application of the basic transform to the source (X, Y) affects V_i separately for $i \in \{0, \dots, M-1\}$, i.e., one can regard the polarization process of the source (X, Y) as a collection of M independent polarization processes $\{(\mathsf{V}_{i,n}, \mathsf{Y}_n) := (V_i^{(B_1)\cdots(B_n)}, Y^{(B_1)\cdots(B_n)})\}_{n=0,1,\dots}$, $i = 0, \dots, M-1$. In this case, if $H(V_i \mid Y)$ is not constant among all $i \in \{0, \dots, M-1\}$, the source $([V_0, \dots, V_{M-1}], Y)$ cannot be polarized in principle. Note that the situation is essentially equivalent to the polar coding for the M-user multiple access channel [9].

C. Sufficiency

In the proof of sufficiency, (X, Y) is assumed to be a symmetric channel. From Lemma 6 we do not lose generality by this assumption. For any $j \in \{0, \dots, \ell-1\}$, it holds via the chain rule for the entropy that

$$\begin{aligned}\sum_{i=j}^{\ell-1} H(X^{(i)} \mid Y^{(i)}) &= H(U_j^{\ell-1} \mid U_0^{j-1}, Y_0^{\ell-1}) \\ &= \sum_{i=j}^{\ell-1} H(U_i \mid U_0^{j-1}, U_{i+1}^{\ell-1}, Y_0^{\ell-1}) \end{aligned} \tag{10}$$

for any (X, Y). Let $\bar{G}$ be an arbitrary standard form of G, and assume that $U_0^{\ell-1}$ and $(X^{(i)}, Y^{(i)})$ for $i \in \{0, \dots, \ell-1\}$ are defined with $\bar{G}$. The Tanner-graph representation of the relationship among $U_0^{\ell-1}$, $X_0^{\ell-1}$ and $Y_0^{\ell-1}$ is shown in Fig. 1(a). All the terms in the sum on the rightmost side of (10) are at most $H(X \mid Y)$ for any symmetric channel (X, Y) on a standard form $\bar{G}$. It also holds that $H(\mathsf{X}_n^{(i)} \mid \mathsf{Y}_n^{(i)}) - H(\mathsf{X}_n \mid \mathsf{Y}_n) \to 0$ with probability 1 as $n \to \infty$ for all $i \in \{0, \dots, \ell-1\}$ since $\{H(\mathsf{X}_n \mid \mathsf{Y}_n)\}_{n=0,1,\dots}$ converges almost surely. Combining these two facts, as well as Lemmas 8 and 9, one observes that each of the terms in the sum on the rightmost side of (10) evaluated with $(X, Y) = (\mathsf{X}_n, \mathsf{Y}_n)$ must be close to $H(\mathsf{X}_n \mid \mathsf{Y}_n)$ with probability 1 as $n \to \infty$. In particular,

$$H(\mathsf{X}_n \mid \mathsf{Y}_n) - H(U_j \mid U_0^{j-1}, U_{j+1}^{\ell-1}, Y_0^{\ell-1})\Big|_{(X,Y)=(\mathsf{X}_n,\mathsf{Y}_n)} \to 0 \tag{11}$$

holds with probability 1. This property allows us to reduce the problem of polarization with G to the properties of the basic transform with $\begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix}$, or equivalently, that with G_γ. Indeed, when one considers the quantity $H(U_j \mid U_0^{j-1}, U_{j+1}^{\ell-1}, Y_0^{\ell-1})\Big|_{(X,Y)=(\mathsf{X}_n,\mathsf{Y}_n)}$, one can safely prune the subgraphs related with the conditioning variables $U_0^{j-1}, U_{j+1}^{\ell-1}$ from Fig. 1(a) to obtain Fig. 1(b) due to Lemma 9, since $(\mathsf{X}_n, \mathsf{Y}_n)$ is always symmetric from Lemma 8. Then, one obtains an upper bound $H(U_j \mid U_0^{j-1}, U_{j+1}^{\ell-1}, Y_i, Y_j)\Big|_{(X,Y)=(\mathsf{X}_n,\mathsf{Y}_n)}$ of $H(U_j \mid U_0^{j-1}, U_{j+1}^{\ell-1}, Y_0^{\ell-1})\Big|_{(X,Y)=(\mathsf{X}_n,\mathsf{Y}_n)}$ for $i < j$. Let γ be the (i, j)-element of $\bar{G}$, and let $\{(\mathsf{X}_n^{(0)}, \mathsf{Y}_n^{(0)}), (\mathsf{X}_n^{(1)}, \mathsf{Y}_n^{(1)})\}$

be the random pairs obtained from $(\mathsf{X}_n, \mathsf{Y}_n)$ via the basic transform with the 2×2 matrix $\begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix}$. Then, the above upper bound is nothing but $H(\mathsf{X}_n^{(1)} \mid \mathsf{Y}_n^{(1)})$. From (11), it holds that $H(\mathsf{X}_n \mid \mathsf{Y}_n) - H(\mathsf{X}_n^{(1)} \mid \mathsf{Y}_n^{(1)}) \to 0$ with probability 1. Therefore, the following proposition implies the sufficiency of the main theorem.

Proposition 14. *Let A be a non-empty subset of $\mathbb{F}_q^\times$. Let $\{(X_{(n)}, Y_{(n)})\}_{n=0,1,\dots}$ be a sequence of random pairs. Assume $H(X_{(n)} \mid Y_{(n)}) - H(X_{(n)}^{(1)} \mid Y_{(n)}^{(1)}) \to 0$ for all G_γ where $\gamma \in A$. Then, for any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that*

$$\begin{aligned} & Z_{td}(X_{(n)} \mid Y_{(n)}) < \epsilon, \qquad \text{for all} \quad t \in \mathbb{F}_p(A)^\times \\ \text{or} \qquad & Z_{td}(X_{(n)} \mid Y_{(n)}) > 1 - \epsilon, \qquad \text{for all} \quad t \in \mathbb{F}_p(A)^\times \end{aligned}$$

for any $n \geq n_0$ and any $d \in \mathbb{F}_q^\times$.

When $\mathbb{F}_p(\bar{G}) = \mathbb{F}_q$, Proposition 14 states that the random sequence $H_n = H(\mathsf{X}_n \mid \mathsf{Y}_n)$ is close to 0 or 1 for sufficiently large n with probability 1. Hence, H_∞ must be $\{0,1\}$-valued, i.e., any source (X, Y) is polarized by G. Proposition 14 is proved by using Lemma 15 and Lemma 16 below.

Lemma 15. *Let $\{(X_{(n)}, Y_{(n)})\}_{n=0,1,\dots}$ be a sequence of random pairs. Assume $H(X_{(n)} \mid Y_{(n)}) - H(X_{(n)}^{(1)} \mid Y_{(n)}^{(1)}) \to 0$ for G_γ where $\gamma \in \mathbb{F}_q^\times$. Then, for any $\epsilon > 0$ there exists $n_0 \in \mathbb{N}$ such that*

$$\begin{aligned} & Z_{\gamma^i d}(X_{(n)} \mid Y_{(n)}) < \epsilon, \qquad \text{for all} \quad i = 0, \dots, q-2 \\ \text{or} \qquad & Z_{\gamma^i d}(X_{(n)} \mid Y_{(n)}) > 1 - \epsilon, \qquad \text{for all} \quad i = 0, \dots, q-2 \end{aligned}$$

for any $n \geq n_0$ and any $d \in \mathbb{F}_q^\times$.

The proof of Lemma 15 is in Appendix A. Lemma 15 means that $\{Z_{\gamma^i d}(X_{(n)} \mid Y_{(n)})\}_{i=0,\dots,q-2}$ are simultaneously close to 0 or 1 for each $d \in \mathbb{F}_q^\times$. Lemma 15 implies Proposition 14 when $A \subseteq \mathbb{F}_q^\times$ includes a primitive element γ of $\mathbb{F}_p(A)$, i.e., $\{\gamma^i \mid i = 0, 1, \dots, q-2\} = \mathbb{F}_p(A)^\times$. If not, we require the following lemma for proving Proposition 14.

Lemma 16 ([4]). *For any d_1 and d_2 in $\mathbb{F}_q^\times$ satisfying $d_2 \neq -d_1$,*

$$\sqrt{1 - Z_{d_1+d_2}(X \mid Y)} \leq \sqrt{1 - Z_{d_1}(X \mid Y)} + \sqrt{1 - Z_{d_2}(X \mid Y)}.$$

Proof: Since

$$1 - Z_d(X \mid Y) = \frac{1}{2} \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathcal{Y}} \left(\sqrt{P_{X,Y}(x, y)} - \sqrt{P_{X,Y}(x + d, y)} \right)^2$$

the statement is obtained from the triangle inequality of the Euclidean distance. ■

Consider partitioning of $\mathbb{F}_q^\times$ according to the equivalence relation $d \sim d' \iff d/d' \in \mathbb{F}_p(A)^\times$. For any fixed $d \in \mathbb{F}_q^\times$, if $Z_d(X_{(n)} \mid Y_{(n)})$ is close to 1, then it follows from Lemma 15 and Lemma 16 that $Z_{d'}(X_{(n)} \mid Y_{(n)})$ is also close to 1 for all $d' \sim d$. Otherwise, all of $\{Z_{d'}(X_{(n)} \mid Y_{(n)})\}_{d' \sim d}$ must not be close to 1, which means from Lemma 15 that all of them must be close to 0. This completes the proof of Proposition 14.

VII. Error probability, total variation distance to the uniform distribution and speed of polarization

A. Preliminaries

In this section, we consider speed of polarization by an $\ell \times \ell$ invertible matrix G over $\mathbb{F}_q$. Let

$$P_{\mathrm{e}}(X \mid Y) := 1 - \sum_{y \in \mathcal{Y}} P_Y(y) \max_{x \in \mathbb{F}_q} P_{X|Y}(x \mid y).$$

This is the average error probability of the maximum a posteriori estimator $\hat{x}(y) := \arg\max_{x \in \mathbb{F}_q} P_{X|Y}(x \mid y)$ of X given Y. The random quantity $P_{\mathrm{e}}(\mathsf{X}_n \mid \mathsf{Y}_n)$ plays a key role in studying speed of polarization. It provides a bound of the block error probability of polar codes with successive cancellation decoding applied to channel coding [3]. More precisely, if one has

$$\Pr(P_{\mathrm{e}}(\mathsf{X}_n \mid \mathsf{Y}_n) < \epsilon) \geq R$$

then it implies existence of a polar code for channel coding with blocklength ℓ^n, rate R, and the block error probability at most $\ell^n R \epsilon$. Obviously, $P_{\mathrm{e}}(X \mid Y)$ is invariant under any permutation of symbols in a posteriori distribution of (X, Y). The average error probability $P_{\mathrm{e}}(X \mid Y)$ takes a value in $[0, (q-1)/q]$. As it has been the case in the study of the binary case [5], the Bhattacharyya parameter is useful for bounding the error probability.

Lemma 17.

$$\frac{q-1}{q^2} \left(\sqrt{1 + (q-1)Z(X \mid Y)} - \sqrt{1 - Z(X \mid Y)} \right)^2 \leq P_{\mathrm{e}}(X \mid Y) \leq \min_{k=1,2,\dots,q-1} \left\{ \frac{(q-1)Z(X \mid Y) + k(k-1)}{k(k+1)} \right\}.$$

Proof of Lemma 17 is in Appendix B.

Another quantity which we study in this section is the expected total variation distance $T(X \mid Y)$ between a posteriori probability and the uniform distribution, defined as

$$T(X \mid Y) := \sum_{y\in\mathcal{Y}} P_Y(y) \sum_{x\in\mathbb{F}_q} \left| P_{X|Y}(x \mid y) - \frac{1}{q} \right|.$$

Properties of the random quantity $T(\mathsf{X}_n \mid \mathsf{Y}_n)$ is important in polar codes for lossy source coding [10], [11]. More precisely, if one has

$$\Pr(T(\mathsf{X}_n \mid \mathsf{Y}_n) < \epsilon) \geq R$$

for the test channel $(\mathsf{X}_0, \mathsf{Y}_0) = (X, Y)$, then there exists a polar code for source coding with blocklength $\ell^n(1-R)$, rate $1-R$ and the average distortion at most $\mathcal{D} + d_{\max}\ell^n R\epsilon$ where $\mathcal{D}$ denotes the average distortion for the test channel and where $d_{\max}$ is the maximum value of the distortion function [10], [11]. Note that $T(X \mid Y)$ is invariant under any permutation of symbols in a posteriori distribution. The total variation distance $T(X \mid Y)$ takes a value in $[0, 2(q-1)/q]$. The following lemma establishes relationship between the total variation distance $T(X \mid Y)$ and the average error probability $P_{\mathrm{e}}(X \mid Y)$.

Lemma 18.

$$2\left(\frac{q-1}{q} - P_{\mathrm{e}}(X \mid Y)\right) \leq T(X \mid Y) \leq \frac{2(q-1)}{q} - \frac{2}{q}\max_{k=1,\dots,q-1}\left\{k(k+1)P_{\mathrm{e}}(X \mid Y) - k(k-1)\right\}$$

The proof is in Appendix C.

The Fourier transform of a posteriori probability is defined for analyzing $T(X \mid Y)$.

Definition 19 (Character)**.** Let $\omega_p \in \mathbb{C}$ be a primitive complex p-th root of unity. Define $\chi(x) := \omega_p^{\mathrm{Tr}(x)}$ for any $x \in \mathbb{F}_q$ where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is defined as $x \mapsto \sum_{j=0}^{m-1} x^{p^j}$. Here, $\mathrm{Tr}(x) \in \mathbb{F}_p$ appearing in the exponent should be regarded as an integer via the natural correspondence between $\mathbb{F}_p$ and $\mathbb{Z}/p\mathbb{Z}$.

From the definition of $\chi(x)$, it satisfies the following properties.

$$\chi(0) = 1, \qquad |\chi(x)| = 1, \text{ for any } x \in \mathbb{F}_q,$$

$$\chi(x+z) = \chi(x)\chi(z), \text{ for any } x, z \in \mathbb{F}_q, \qquad \sum_{x\in\mathbb{F}_q} \chi(x) = 0.$$

In this paper, we only use $\chi(x)$ through these properties.

Definition 20 (Fourier transform)**.** For any fixed $y \in \mathcal{Y}$, the Fourier transform of the a posteriori probability $P_{X|Y}$ of a source (X, Y) is defined as

$$P^*_{X|Y}(w \mid y) := \sum_{z\in\mathbb{F}_q} P_{X|Y}(z \mid y)\chi(wz)$$

for $w \in \mathbb{F}_q$.

Note that $P^*_{X|Y}(0 \mid y) = 1$ for any $y \in \mathcal{Y}$. Like the role of $Z(X \mid Y)$ in studying $P_{\mathrm{e}}(X \mid Y)$, the auxiliary quantity $S(X \mid Y)$, defined as

$$S(X \mid Y) := \frac{1}{q-1}\sum_{w\in\mathbb{F}_q^\times}\sum_{y\in\mathcal{Y}} P_Y(y)\left|P^*_{X|Y}(w \mid y)\right|$$

can be used for analyzing $T(X \mid Y)$. The quantity $S(X \mid Y)$ takes a value in $[0,1]$. Note that, although $S(X \mid Y)$ is identical to $T(X \mid Y)$ (and $1 - 2P_{\mathrm{e}}(X \mid Y)$) when $q = 2$, $S(X \mid Y)$ is in general different from $T(X \mid Y)$. In this regard, consideration of the quantity $S(X \mid Y)$ is a novel idea that comes into play when one considers non-binary cases. Although $S(X \mid Y)$ is *not* invariant under any permutation of symbols in a posteriori distribution, $S(X \mid Y)$ is invariant under a permutation of symbols in a posteriori distribution when the permutation is addition or multiplication on the finite field i.e., $S(X \mid Y) = S(r(Y)X + d(Y) \mid Y)$ for any $d : \mathcal{Y} \to \mathbb{F}_q$ and $r : \mathcal{Y} \to \mathbb{F}_q^\times$. Hence, if $(X, Y) \overset{\mathrm{a}}{\sim} (X', Y')$, it holds that $S(X \mid Y) = S(X' \mid Y')$.

The following lemma relates the quantity $S(X \mid Y)$ with the average error probability $P_{\mathrm{e}}(X \mid Y)$.

Lemma 21.

$$\begin{aligned} 1 - \frac{q}{q-1}P_{\mathrm{e}}(X \mid Y) &\leq S(X \mid Y) \\ &\leq \min_{k=1,\dots,q-1}\left\{k(k+1)\left[\left(\frac{k}{k+1} - P_{\mathrm{e}}(X \mid Y)\right)\sqrt{1 - \frac{q}{q-1}\frac{k-1}{k}} + \left(P_{\mathrm{e}}(X \mid Y) - \frac{k-1}{k}\right)\sqrt{1 - \frac{q}{q-1}\frac{k}{k+1}}\right]\right\}. \end{aligned}$$

The proof is in Appendix D.

We now define the following equivalence relation for establishing relationship among several quantities for a source (X,Y) defined so far.

Definition 22. For $A(X \mid Y) \in [0,1]$ and $B(X \mid Y) \in [0,1]$, we say $A(X \mid Y) \overset{\mathrm{p}}{\sim} B(X \mid Y)$ if and only if there exists $\epsilon > 0$ and $c \in (0,1]$ such that if $B(X \mid Y) < \epsilon$,

$$B(X \mid Y)^{\frac{1}{c}} \le A(X \mid Y) \le B(X \mid Y)^{c}$$

and if $1 - B(X \mid Y) < \epsilon$,

$$(1 - B(X \mid Y))^{\frac{1}{c}} \le 1 - A(X \mid Y) \le (1 - B(X \mid Y))^{c}$$

for any source (X,Y).

From Lemmas 17, 18 and 21, the following corollary is obtained.

Corollary 23. $(q/(q-1))P_{\mathrm{e}}(X \mid Y) \overset{\mathrm{p}}{\sim} Z(X \mid Y) \overset{\mathrm{p}}{\sim} 1 - (q/(2(q-1)))T(X \mid Y) \overset{\mathrm{p}}{\sim} 1 - S(X \mid Y)$.

The following four quantities are used in the derivation of the speed of polarization in the next subsection.

Definition 24. For any channel (X,Y), $Z_{\max}(X,Y)$ and $Z_{\min}(X,Y)$ are defined as

$$Z_{\max}(X,Y) := \max_{\substack{x \in \mathbb{F}_q, x' \in \mathbb{F}_q \\ x \neq x'}} \sum_{y \in \mathcal{Y}} \sqrt{P_{Y|X}(y \mid x) P_{Y|X}(y \mid x')}$$

$$Z_{\min}(X,Y) := \min_{x \in \mathbb{F}_q, x' \in \mathbb{F}_q} \sum_{y \in \mathcal{Y}} \sqrt{P_{Y|X}(y \mid x) P_{Y|X}(y \mid x')}.$$

For any source (X,Y), $S_{\max}(X,Y)$ and $S_{\min}(X,Y)$ are defined as

$$S_{\max}(X,Y) := \max_{w \in \mathbb{F}_q^{\times}} \sum_{y \in \mathcal{Y}} P_Y(y) \left| P^{*}_{X|Y}(w \mid y) \right|$$

$$S_{\min}(X,Y) := \min_{w \in \mathbb{F}_q^{\times}} \sum_{y \in \mathcal{Y}} P_Y(y) \left| P^{*}_{X|Y}(w \mid y) \right|.$$

The quantities $Z_{\max}(X,Y)$ and $Z_{\min}(X,Y)$ are invariant under any permutation of symbols in a posteriori distribution. Although $S_{\max}(X,Y)$ and $S_{\min}(X,Y)$ are *not* invariant under any permutation of symbols in a posteriori distribution, it holds that $S_{\max/\min}(X \mid Y) = S_{\max/\min}(rX + d(Y) \mid Y)$ for any $d : \mathcal{Y} \to \mathbb{F}_q$ and $r \in \mathbb{F}_q^{\times}$. Hence, if $(X,Y) \overset{\mathrm{a}}{\sim} (X',Y')$, it holds that $S_{\max/\min}(X \mid Y) = S_{\max/\min}(X' \mid Y')$. It is also straightforward to see the inequalities $Z_{\min}(X,Y) \le Z(X \mid Y) \le Z_{\max}(X,Y)$ and $S_{\min}(X,Y) \le S(X \mid Y) \le S_{\max}(X,Y)$ to hold.

B. Speed of polarization

In this subsection, we assume that $H(X \mid Y) \in (0,1)$, and also assume in view of Lemma 6, without loss of generality, that (X,Y) is a channel. The following theorem holds, which was shown by Arıkan and Telatar [12], Korada et al. [5] and Korada [13] for the binary case with an additional condition.

Theorem 25. *If a channel (X,Y) is polarized by G, it holds that for any $\epsilon > 0$,*

$$\begin{aligned} &\lim_{n\to\infty} \Pr\left(P_{\mathrm{e}}(\mathsf{X}_n \mid \mathsf{Y}_n) < 2^{-\ell^{(E_{\mathrm{c}}(G)-\epsilon)n}} \right) = 1 - H(X \mid Y) \\ &\lim_{n\to\infty} \Pr\left(P_{\mathrm{e}}(\mathsf{X}_n \mid \mathsf{Y}_n) < 2^{-\ell^{(E_{\mathrm{c}}(G)+\epsilon)n}} \right) = 0 \end{aligned} \tag{12}$$

where

$$E_{\mathrm{c}}(G) := \frac{1}{\ell \log \ell} \sum_{i=0}^{\ell-1} \log D_{\mathrm{c}}^{(i)}(G)$$

is the quantity called the exponent of G for channel coding, and where $D_{\mathrm{c}}^{(i)}(G)$ denotes Hamming distance between i-th row of G and the linear space spanned by $(i+1)$-th row to $(\ell-1)$-th row of G. Furthermore, it holds that for any $\epsilon > 0$,

$$\begin{aligned} &\lim_{n\to\infty} \Pr\left(T(\mathsf{X}_n \mid \mathsf{Y}_n) < 2^{-\ell^{(E_{\mathrm{s}}(G)-\epsilon)n}} \right) = H(X \mid Y) \\ &\lim_{n\to\infty} \Pr\left(T(\mathsf{X}_n \mid \mathsf{Y}_n) < 2^{-\ell^{(E_{\mathrm{s}}(G)+\epsilon)n}} \right) = 0, \end{aligned} \tag{13}$$

where

$$E_{\mathrm{s}}(G) := \frac{1}{\ell \log \ell} \sum_{i=0}^{\ell-1} \log D_{\mathrm{s}}^{(i)}(G)$$

is the quantity called the exponent of G for source coding, and where $D_{\mathrm{s}}^{(i)}(G)$ denotes Hamming distance between i-th column of G^{-1} and the linear space spanned by 0-th column to $(i-1)$-th column of G^{-1}.

Remark 1. Korada proved (13) for the binary case with the aid of the condition $D_{\mathrm{s}}^{(i)}(G) \geq D_{\mathrm{s}}^{(i+1)}(G)$ for $i = 0, \dots, \ell-2$ [13]. In this paper, (13) is proved without any additional condition for both binary and non-binary cases.

From Theorem 25, the error probability of polar code as channel code of rate smaller than $I(W)$ and the distortion gap to the optimal distortion of polar codes as source code are asymptotically bounded by $2^{-\ell^{(E_{\mathrm{c}}(G)-\epsilon)n}}$ and $2^{-\ell^{(E_{\mathrm{s}}(G)-\epsilon)n}}$, respectively [13]. From Corollary 23, it is sufficient to prove (12) and (13) for $Z(\mathsf{X}_n \mid \mathsf{Y}_n)$ and $S(\mathsf{X}_n \mid \mathsf{Y}_n)$ instead of $P_{\mathrm{e}}(\mathsf{X}_n \mid \mathsf{Y}_n)$ and $T(\mathsf{X}_n \mid \mathsf{Y}_n)$, respectively. The general proof shown in [14], [15] can be used for our purpose.

Lemma 26 ([14], [15])**.** *Let $\{Z_n\}_{n=0,1,\dots}$ be a random process ranging in $[0,1]$ and $\{D_n\}_{n=0,1,\dots}$ be i.i.d. random variables ranging in $[1,\infty)$. Assume that the expectation of $\log D_0$ exists. Four conditions (c0)–(c3) are defined as follows.*

(c0) *$Z_n \in (0,1)$ with probability 1.*
(c1) *There exists a random variable Z_∞ such that $Z_n \to Z_\infty$ almost surely.*
(c2) *There exists a positive constant c_0 such that $Z_{n+1} \leq c_0 Z_n^{D_n}$ with probability 1.*
(c3) *$Z_n^{D_n} \leq Z_{n+1}$ with probability 1.*

If (c0), (c1) and (c2) are satisfied, it holds that

$$\lim_{n\to\infty} \Pr\left(Z_n < 2^{-\ell^{(\mathbb{E}[\log_\ell D_0]-\epsilon)n}}\right) = \Pr(Z_\infty = 0). \tag{14}$$

If (c0), (c1) and (c3) are satisfied, it holds that

$$\lim_{n\to\infty} \Pr\left(Z_n < 2^{-\ell^{(\mathbb{E}[\log_\ell D_0]+\epsilon)n}}\right) = 0. \tag{15}$$

In the above, ℓ is any constant greater than 1.

Theorem 25 is proved by applying Lemma 26 to appropriate pairs of random processes. The first equation of (12) is proved by confirming that the pair of the random processes $\{Z_n = Z_{\max}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{c}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the conditions (c0), (c1) and (c2) and then by applying (14). The first equation of (13) is proved in the same way, by observing that the pair of the processes $\{Z_n = S_{\max}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{s}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the conditions (c0), (c1) and (c2) and then by applying (14). The proof of the second equation of (12) is obtained similarly, by confirming that the pair of the processes $\{Z_n = Z_{\min}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{c}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the conditions (c0), (c1) and (c3) and then by applying (15). For the proof of the second equation of (13), one should confirm that the pair of the processes $\{Z_n = S_{\min}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{s}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the conditions (c0), (c1) and (c3) and then apply (15).

From Lemma 13 and Corollary 23, the condition (c1) is satisfied by $Z_n = Z_{\max}(\mathsf{X}_n, \mathsf{Y}_n)$, $Z_{\min}(\mathsf{X}_n, \mathsf{Y}_n)$, $S_{\max}(\mathsf{X}_n, \mathsf{Y}_n)$ and $S_{\max}(\mathsf{X}_n, \mathsf{Y}_n)$ when a channel (X, Y) is polarized by G. In these cases, it holds that $Z_\infty \in \{0,1\}$ with probability 1, and that $\Pr(Z_\infty = 0) = 1 - H(X \mid Y)$ for $Z_n = Z_{\max}(\mathsf{X}_n, \mathsf{Y}_n)$ and $Z_{\min}(\mathsf{X}_n, \mathsf{Y}_n)$, and $\Pr(Z_\infty = 0) = H(X \mid Y)$ for $Z_n = S_{\max}(\mathsf{X}_n, \mathsf{Y}_n)$ and $S_{\min}(\mathsf{X}_n, \mathsf{Y}_n)$. The following lemma shows that the pair of $\{Z_n = Z_{\max}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{c}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the condition (c2), and that the pair of $\{Z_n = Z_{\min}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{c}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the condition (c3).

Lemma 27 ([5])**.** *For $i \in \{0, \dots, \ell-1\}$, it holds for any channel (X, Y) that*

$$Z_{\max}(X^{(i)}, Y^{(i)}) \leq q^{\ell-1-i} Z_{\max}(X, Y)^{D_{\mathrm{c}}^{(i)}(G)}$$
$$Z_{\min}(X, Y)^{D_{\mathrm{c}}^{(i)}(G)} \leq Z_{\min}(X^{(i)}, Y^{(i)}).$$

The proof is omitted since the same proof for the binary alphabet in [5] applies to the non-binary cases as well. The following lemma shows that the pair of $\{Z_n = S_{\max}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{s}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the condition (c2), and that the pair of $\{Z_n = S_{\min}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{s}}^{(B_n)}(G)\}_{n=0,1,\dots}$ satisfies the condition (c3).

Lemma 28. *For $i \in \{0, \dots, \ell-1\}$, it holds for any source (X, Y) that*

$$S_{\max}(X^{(i)}, Y^{(i)}) \leq q^{i} S_{\max}(X, Y)^{D_{\mathrm{s}}^{(i)}(G)}$$
$$S_{\min}(X, Y)^{D_{\mathrm{s}}^{(i)}(G)} \leq S_{\min}(X^{(i)}, Y^{(i)}).$$

The proof is in Appendix E. Since $S_{\max}(X, Y) = 1 \iff S(X \mid Y) = 1$, it always holds that $S_{\max}(X, Y) < 1$ and hence the condition (c0) is satisfied by the pair of $\{Z_n = S_{\max}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{s}}^{(B_n)}(G)\}_{n=0,1,\dots}$. Hence, the first equality in (13) is proved by applying Lemma 26 to the pair of $\{Z_n = S_{\max}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{s}}^{(B_n)}(G)\}_{n=0,1,\dots}$. When $0 < S_{\min}(X, Y)$, the condition (c0) is satisfied by the pair of $\{Z_n = S_{\min}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{s}}^{(B_n)}(G)\}_{n=0,1,\dots}$, and hence (15) can be applied to the pair to prove the second equality in (13). When $0 < Z_{\min}(X, Y) \le Z_{\max}(X, Y) < 1$, (14) and (15) can be applied to the pair of $\{Z_n = Z_{\max}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{c}}^{(B_n)}(G)\}_{n=0,1,\dots}$, and to the pair of $\{Z_n = Z_{\min}(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ and $\{D_n = D_{\mathrm{c}}^{(B_n)}(G)\}_{n=0,1,\dots}$, respectively, since the pairs satisfy the condition (c0), which proves (12). For the other cases, it is sufficient to prove the following lemma.

Lemma 29.

$$\lim_{n\to\infty} \Pr\left(Z_{\min}(\mathsf{X}_n, \mathsf{Y}_n) > 0, Z_{\max}(\mathsf{X}_n, \mathsf{Y}_n) < 1\right) = 1$$

$$\lim_{n\to\infty} \Pr\left(S_{\min}(\mathsf{X}_n, \mathsf{Y}_n) > 0\right) = 1$$

Proof: For the first equation, let us consider a $\sigma(B_1, \dots, B_n)$-measurable random process $\{\xi_n := \xi(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ where

$$\xi(X, Y) := \left(\left\{(x, x') \in \mathbb{F}_q^2 \mid Z_{x,x'}(X \mid Y) = 0\right\}, \left\{(x, x') \in \mathbb{F}_q^2 \mid Z_{x,x'}(X \mid Y) = 1\right\}\right)$$

and where

$$Z_{x,x'}(X \mid Y) := \sum_{y\in\mathcal{Y}} \sqrt{P_{Y|X}(y \mid x) P_{Y|X}(y \mid x')}.$$

Then, $\{\xi_n\}_{n=0,1,\dots}$ is obviously a Markov chain. The Markov chain $\{\xi_n\}_{n=0,1,\dots}$ has the absorbing state (ϕ, ϕ), i.e., $\Pr(\xi_n = (\phi, \phi) \mid \xi_{n-1} = (\phi, \phi)) = 1$. Although there are two other absorbing states $(\{(x, x') \in \mathbb{F}_q^2 \mid x \ne x'\}, \{(x, x') \in \mathbb{F}_q^2 \mid x = x'\})$ and $(\phi, \mathbb{F}_q^2)$, these states are isolated, i.e., these states are not accessible from other states. From any state which is accessible from the initial state ξ_0, (ϕ, ϕ) is accessible both since any source accessible from the original source (X, Y) by G is also polarized by G, and since once a source satisfies $Z_{\max}(\mathsf{X}_{n-1}, \mathsf{Y}_{n-1}) < 1$ or $Z_{\min}(\mathsf{X}_{n-1}, \mathsf{Y}_{n-1}) > 0$, the offspring sources also satisfy $Z_{\max}(\mathsf{X}_n, \mathsf{Y}_n) < 1$ or $Z_{\min}(\mathsf{X}_n, \mathsf{Y}_n) > 0$, respectively. Hence, $\lim_{n\to\infty} \Pr(\xi_n = (\phi, \phi)) = 1$, proving the first equation of the lemma.

The second equation is obtained in the same way. Let us define

$$S_w(X \mid Y) := \sum_{y\in\mathcal{Y}} P_Y(y) \left| P^*_{X|Y}(w \mid y) \right|$$

and let $\{\eta_n := \eta(\mathsf{X}_n, \mathsf{Y}_n)\}_{n=0,1,\dots}$ be a $\sigma(B_1, \dots, B_n)$-measurable random process where

$$\eta(X, Y) := (\{w \in \mathbb{F}_q \mid S_w(X \mid Y) = 0\}).$$

Then, $\{\eta_n\}_{n=0,1,\dots}$ is a Markov chain since one obtains from the derivations of (25) and (26) in Appendix E that

$$\max_{z_0^{\ell-1} \in \mathcal{C}_i(w)} \prod_{j=0}^{\ell-1} S_{z_j}(X \mid Y) \le S_w(X^{(i)} \mid Y^{(i)}) \le q^i \max_{z_0^{\ell-1} \in \mathcal{C}_i(w)} \prod_{j=0}^{\ell-1} S_{z_j}(X \mid Y)$$

for any $w \in \mathbb{F}_q^\times$ and $i = 0, \dots, \ell - 1$ where $\mathcal{C}_i(w)$ is the affine space $\{\sum_{j=0}^{i-1} a_j h_j^t + w h_i^t \mid a_0^{i-1} \in \mathbb{F}_q^i\}$ defined on the basis of the columns of $G^{-1} := [h_0, h_1, \dots, h_{\ell-1}]$. The superscript ^{t} here denotes transpose of a vector. Then, it holds that $\lim_{n\to\infty} \Pr(\eta_n = \phi) = 1$ due to the same reason as that for $\{\xi_n\}_{n=0,1,\dots}$. ■

A more detailed asymptotic analysis depending on the rate can also be performed as shown in [16], [17], [14], [15] for the binary case. For example, under the condition that G polarizes (X, Y), one can prove that for $R \in (0, 1 - H(X \mid Y))$,

$$\lim_{n\to\infty} \Pr\left(P_{\mathrm{e}}(\mathsf{X}_n \mid \mathsf{Y}_n) < 2^{-\ell^{E_{\mathrm{c}}(G)n + \sqrt{V_{\mathrm{c}}(G)n}\,Q^{-1}\left(\frac{R}{1-H(X|Y)}\right) + f(n)}}\right) = R \tag{16}$$

holds for an arbitrary function satisfying $f(n) = o(\sqrt{n})$, where

$$V_{\mathrm{c}}(G) := \frac{1}{\ell} \sum_{i=0}^{\ell-1} (\log_\ell D_{\mathrm{c}}^{(i)}(G) - E_{\mathrm{c}}(G))^2$$

and where $Q^{-1}(\cdot)$ is the inverse function of the error function $Q(t) := \int_t^\infty e^{-z^2/2}\, dz / \sqrt{2\pi}$.

In the binary case, any source is polarized by G if and only if $E_{\mathrm{c}}(G) > 0$ [5]. The property also holds when q is a prime since the condition $E_{\mathrm{c}}(G) > 0$ is equivalent to the condition that a standard form of G is not the identity matrix. However, it no longer holds when q is not a prime, in which case there may be sources which are not polarized by G even if $E_{\mathrm{c}}(G) > 0$, as shown in Section VI-B. Since non-zero scalar multiplication of a column does not change the exponent $E_{\mathrm{c}}(G)$, even if there are non-polarizing sources for G satisfying $E_{\mathrm{c}}(G) > 0$, appropriate scalar multiplication of a column of G gives a matrix with the same exponent $E_{\mathrm{c}}(G)$ which polarizes any source.

VIII. Reed-Solomon matrix and its exponent

Let $\mathbb{F}_q = \{x_0, \dots, x_{q-1}\}$. Let $a = [a_0, \dots, a_{k-1}] \in \mathbb{F}_q^k$ and $p_a(X) = a_0 + a_1 X + \cdots + a_{k-1}X^{k-1}$. The encoder of the q-ary extended Reed-Solomon code is defined as $\varphi(a) := [p_a(x_0), p_a(x_1), \dots, p_a(x_{q-1})]$. Let α be a primitive element of $\mathbb{F}_q$. When $x_{q-1} = 0$ and $x_i = \alpha^{-i}$ for $i = 0, \dots, q-2$, the generator matrix of the q-ary extended Reed-Solomon code is a lower submatrix of the $q \times q$ matrix $G_{\mathrm{RS}}(q)$ over $\mathbb{F}_q$ which we call the Reed-Solomon matrix

$$G_{\mathrm{RS}}(q) := \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} & 0 \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & \alpha^{q-2} & \alpha^{2(q-2)} & \cdots & \alpha^{(q-2)(q-2)} & 0 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}.$$

From Theorem 11, any source is polarized by the Reed-Solomon matrix. Since extended Reed-Solomon codes are maximum distance separable (MDS) codes, one has $D_{\mathrm{c}}^{(i)} = i + 1$ for $i = 0, \dots, q-1$, and therefore the exponent of the Reed-Solomon matrix for channel coding is $E_{\mathrm{c}}(G_{\mathrm{RS}}(q)) = \log(q!)/q$. The inverse matrix of the Reed-Solomon matrix $G_{\mathrm{RS}}(q)$ is

$$G_{\mathrm{RS}}(q)^{-1} = - \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(q-2)} & 0 \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(q-2)} & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & \alpha^{-(q-2)} & \alpha^{-2(q-2)} & \cdots & \alpha^{-(q-2)(q-2)} & 0 \\ 1 & 0 & 0 & \cdots & 0 & -1 \end{bmatrix}.$$

Hence, the exponent of the Reed-Solomon matrix for source coding is also $E_{\mathrm{s}}(G_{\mathrm{RS}}(q)) = \log(q!)/q$. Note that both the exponents $\log(q!)/q$ monotonically increases in q and converges to 1 as $q \to \infty$.

For $i \in \{0, 1, \dots, q^n - 1\}$, $i_n i_{n-1} \cdots i_1$ denotes the q-ary expansion of i. For polar codes constructed on the basis of the matrix $G_{\mathrm{RS}}(q)$, rows of $G_{\mathrm{RS}}(q)^{\otimes n}$ whose indices are in the set

$$\{i \in \{0, \dots, q^n - 1\} \mid H(X^{(i_1)\cdots(i_n)} \mid Y^{(i_1)\cdots(i_n)}) < \epsilon\}$$

with some threshold $\epsilon > 0$ are chosen, as mentioned in Section III-B. For the Reed-Muller codes, on the other hand, rows of $G_{\mathrm{RS}}(q)^{\otimes n}$ whose indices belong to

$$\{i \in \{0, \dots, q^n - 1\} \mid i_1 + \cdots + i_n > n_0\}$$

are chosen for some threshold $n_0 \in \{0, 1, \dots, n(q-1)\}$[3]. In order to maximize the minimum distance, rows of $G_{\mathrm{RS}}(q)^{\otimes n}$ with indices in the set

$$\{i \in \{0, \dots, q^n - 1\} \mid (i_1 + 1) \cdots (i_n + 1) > n_0\}. \tag{17}$$

with some threshold $n_0 \in \{1, 2, \dots, q^n\}$ should be chosen. Hence, unless $q = 2$, the selection rule for the Reed-Muller codes does not maximize the minimum distance. Codes based on the selection rule (17) are sometimes called Massey-Costello-Justesen codes [18] and hyperbolic cascaded Reed-Solomon codes [19]. Note that the minimum distance of Reed-Muller codes grows like $q^{n/2+o(n)}$ while the minimum distance of polar codes and hyperbolic codes grows like $q^{E_{\mathrm{c}}(G_{\mathrm{RS}}(q))n+o(n)}$. From the above observation, the Reed-Solomon matrix can be regarded as a natural generalization of the matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ in the binary case.

We now consider the maximum exponent $E_{\max}(q, \ell) := \max_{G \in \mathbb{F}_q^{\ell \times \ell}} E_{\mathrm{c}}(G)$ for channel coding on given size q of a finite field and size ℓ of a matrix. For $q = 2$, Korada et al. [5] show that $E_{\max}(2, \ell) < 0.55$ for $\ell \leq 31$, and also show a method of construction of binary matrices with large exponents using the BCH codes. For $q \geq 2$ and $\ell \leq q$, the $\ell \times \ell$ lower-right submatrix of the q-ary Reed-Solomon matrix gives the largest exponent so that $E_{\max}(q, \ell) = \log(\ell!)/(\ell \log \ell)$ for $\ell \leq q$ since the Reed-Solomon code is an MDS code [20]. Thus, the Reed-Solomon matrices with $q > 2$ can be regarded as providing a systematic means to construct polar codes with larger exponents for the case $\ell \leq q$. For example, for $q = 4$, $E_{\max}(4, 4) = E_{\mathrm{c}}(G_{\mathrm{RS}}(4)) \approx 0.573\,12$, which is larger than the upper bound 0.55 of $E_{\max}(2, \ell)$ for $\ell \leq 31$. For $\ell > q > 2$, on the other hand, algebraic geometry codes are considered to be useful since they have a large minimum distance and the nested structure which are plausible in making $D_{\mathrm{c}}^{(i)}$s larger. The examples using the Hermitian codes are shown in [2], in which $q = p^m$ and $\ell = p^{3m/2}$ for an even integer m. The q-ary $\ell \times \ell$ matrix constructed on the basis of the Hermitian code has a yet larger exponent than the Reed-Solomon matrix $G_{\mathrm{RS}}(q)$ for $q > 4$.

[3] Here, $i_1, \dots, i_n$ are treated as integers in the additions.

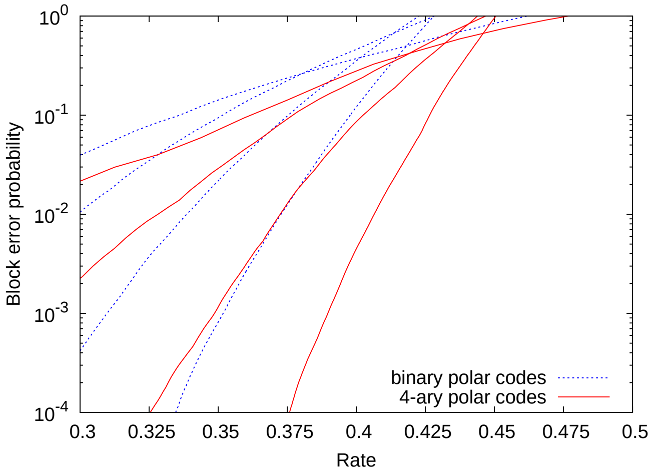


Fig. 2. Numerical results on the upper bound of the block error probability of polar codes over an AWGN channel, for which the standard deviation of noise is set equal to 0.978 65. The capacity of the AWGN channel is about 0.5. Results of binary polar codes and quaternary polar codes using $G_{\mathrm{RS}}(4)$ are shown by dotted curves and solid curves, respectively. Blocklengths are 2^7, 2^9, 2^{11}, and 2^{13} viewed as binary codes.

IX. Numerical results

In Fig. 2, performances of the original binary polar codes with G_1 and quaternary polar codes using the Reed-Solomon matrix $G_{\mathrm{RS}}(4)$ are compared on the binary-input AWGN channel with capacity about 0.5. Instead of the actual error probability, the upper bound $\sum_{i\in\mathcal{A}} P_{\mathrm{e}}(X^{(i_1)\cdots(i_n)} \mid Y^{(i_1)\cdots(i_n)})$ is plotted where $\mathcal{A}$ denotes the set of chosen row indices in constructing polar codes. This bound is accurate for rates not close to the capacity [21]. A significant improvement by the quaternary polar codes over the binary counterparts is observed in terms of the block error probability, although the error probability of the quaternary polar codes is still larger than that of (3,6)-regular LDPC codes except in a low-rate region.

X. Summary

We have shown that a necessary and sufficient condition for a q-ary $\ell\times\ell$ invertible matrix G over $\mathbb{F}_q$ with a non-identity standard form $\bar{G}$ to polarize any source/channel is $\mathbb{F}_p(\bar{G}) = \mathbb{F}_q$. The result about speed of polarization for the binary alphabet has been generalized to non-binary cases. We have also explicitly given q-ary $\ell\times\ell$ matrices with $\ell \le q$ on the basis of the q-ary Reed-Solomon matrices, which have the largest exponent $E_{\max}(q,\ell) = \log(\ell!)/(\ell\log\ell)$ among all $\ell\times\ell$ matrices. Performances of non-binary polar codes based on Reed-Solomon matrices are found via numerical evaluation to be significantly better than the performance of the original binary polar codes.

Appendix A
Proof of Lemma 15

In order to relate the entropy and the Bhattacharyya parameter, the following lemma is useful.

Lemma 30 ([22]). *For any random variables X, Y and Z on sets $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, respectively,*

$$\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_{X,Y}(x,y)\log\frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)} \ge -\log\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}} P_X(x)\sqrt{P_{Y|X}(y\mid x)}\right)^2$$

$$\sum_{x\in\mathcal{X},y\in\mathcal{Y},z\in\mathcal{Z}} P_{X,Y,Z}(x,y,z)\log\frac{P_{X,Y|Z}(x,y\mid z)}{P_{X|Z}(x\mid z)P_{Y|Z}(y\mid z)} \ge -\log\sum_{y\in\mathcal{Y},z\in\mathcal{Z}} P_Z(z)\left(\sum_{x\in\mathcal{X}} P_{X|Z}(x\mid z)\sqrt{P_{Y|X,Z}(y\mid x,z)}\right)^2.$$

Proof: The second inequality is an immediate consequence of the first inequality and Jensen's inequality. The first inequality is obtained by using Jensen's inequality twice as follows.

$$\begin{aligned}\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_{X,Y}(x,y)\log\frac{P_{X,Y}(x,y)}{P_X(x)P_Y(y)} &= -2\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_{X,Y}(x,y)\log\sqrt{\frac{P_X(x)P_Y(y)}{P_{X,Y}(x,y)}}\\ &\geq -2\sum_{y\in\mathcal{Y}} P_Y(y)\log\sum_{x\in\mathcal{X}} P_{X|Y}(x\mid y)\sqrt{\frac{P_X(x)P_Y(y)}{P_{X,Y}(x,y)}}\\ &= -\sum_{y\in\mathcal{Y}} P_Y(y)\log\left(\sum_{x\in\mathcal{X}} P_{X|Y}(x\mid y)\sqrt{\frac{P_X(x)P_Y(y)}{P_{X,Y}(x,y)}}\right)^2\\ &\geq -\log\sum_{y\in\mathcal{Y}} P_Y(y)\left(\sum_{x\in\mathcal{X}} P_{X|Y}(x\mid y)\sqrt{\frac{P_X(x)P_Y(y)}{P_{X,Y}(x,y)}}\right)^2\\ &= -\log\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}} P_X(x)\sqrt{P_{Y|X}(y\mid x)}\right)^2.\end{aligned}$$

■

In Lemma 30, the quantities on the left-hand sides are the mutual information between X and Y, and the conditional mutual information between X and Y given Z, respectively. The quantities on the right-hand sides are the cutoff rate and the conditional cutoff rate, respectively.

Given a source (X, Y), let $(U_0, U_1, X_0, X_1, Y_0, Y_1)$ be the random variables defined by applying the basic transform with G_γ to the source (X, Y), as described in Section III. Then, one obtains

$$\begin{aligned}&H(U_1\mid Y_1) - H(U_1\mid U_0,Y_0,Y_1)\\ &= \sum_{u_0\in\mathbb{F}_q,u_1\in\mathbb{F}_q,y_0\in\mathcal{Y},y_1\in\mathcal{Y}} P_{U_0,U_1,Y_0,Y_1}(u_0,u_1,y_0,y_1)\log\frac{P_{U_0,U_1,Y_0|Y_1}(u_0,u_1,y_0\mid y_1)}{P_{U_1|Y_1}(u_1\mid y_1)P_{U_0,Y_0|Y_1}(u_0,y_0\mid y_1)}\\ &\geq -\log\left[\sum_{y_1\in\mathcal{Y}} P_Y(y_1)\sum_{u_0\in\mathbb{F}_q,y_0\in\mathcal{Y}}\left[\sum_{u_1\in\mathbb{F}_q} P_{U_1|Y_1}(u_1\mid y_1)\sqrt{P_{U_0,Y_0|U_1,Y_1}(u_0,y_0\mid u_1,y_1)}\right]^2\right]\\ &= -\log\left[\sum_{y_1\in\mathcal{Y}} P_Y(y_1)\sum_{u_0\in\mathbb{F}_q,y_0\in\mathcal{Y}}\left[\sum_{u_1\in\mathbb{F}_q} P_{U_1|Y_1}(u_1\mid y_1)\sqrt{P_{X_0,Y_0}(u_0+u_1,y_0)}\right]^2\right]\\ &= -\log\left[\sum_{y_1\in\mathcal{Y}} P_Y(y_1)\sum_{u_1\in\mathbb{F}_q,u_1'\in\mathbb{F}_q} P_{X|Y}(\gamma u_1\mid y_1)P_{X|Y}(\gamma u_1'\mid y_1)\sum_{u_0\in\mathbb{F}_q,y_0\in\mathcal{Y}}\sqrt{P_{X,Y}(u_0+u_1,y_0)}\sqrt{P_{X,Y}(u_0+u_1',y_0)}\right]\\ &= -\log\left[1-\sum_{y_1\in\mathcal{Y}} P_Y(y_1)\sum_{u_1\in\mathbb{F}_q,u_1'\in\mathbb{F}_q} P_{X|Y}(\gamma u_1\mid y_1)P_{X|Y}(\gamma u_1'\mid y_1)\right.\\ &\qquad\left.\cdot\left(1-\sum_{u_0\in\mathbb{F}_q,y_0\in\mathcal{Y}}\sqrt{P_{X,Y}(u_0+u_1,y_0)}\sqrt{P_{X,Y}(u_0+u_1',y_0)}\right)\right]\\ &= -\log\left[1-q\sum_{d\in\mathbb{F}_q}\sum_{y_1\in\mathcal{Y}} P_Y(y_1)\sum_{u_1\in\mathbb{F}_q}\frac{1}{q}P_{X|Y}(\gamma u_1\mid y_1)P_{X|Y}(\gamma u_1+\gamma d\mid y_1)\right.\\ &\qquad\left.\cdot\left(1-\sum_{u_0\in\mathbb{F}_q,y_0\in\mathcal{Y}}\sqrt{P_{X,Y}(u_0+u_1,y_0)}\sqrt{P_{X,Y}(u_0+u_1+d,y_0)}\right)\right]\\ &\geq -\log\left[1-q\sum_{d\in\mathbb{F}_q^\times}\left(\sum_{u_1\in\mathbb{F}_q,y_1\in\mathcal{Y}}\frac{1}{q}P_Y(y_1)\sqrt{P_{X|Y}(\gamma u_1\mid y_1)P_{X|Y}(\gamma u_1+\gamma d\mid y_1)}\right)^2\right.\\ &\qquad\left.\cdot\left(1-\sum_{u_0\in\mathbb{F}_q,y_0\in\mathcal{Y}}\sqrt{P_{X,Y}(u_0,y_0)}\sqrt{P_{X,Y}(u_0+d,y_0)}\right)\right]\\ &= -\log\left[1-\frac{1}{q}\sum_{d\in\mathbb{F}_q^\times} Z_{\gamma d}(X\mid Y)^2(1-Z_d(X\mid Y))\right].\end{aligned}$$

The first and second inequalities are obtained by Lemma 30 and Jensen's inequality, respectively.

The assumption of Lemma 15 implies that the above formula evaluated for $(X,Y) = (X_{(n)}, Y_{(n)})$ approaches 0 as $n \to \infty$, or equivalently, that for any $\epsilon > 0$, there exists n_0 such that

$$Z_{\gamma d}(X_{(n)} \mid Y_{(n)})(1 - Z_d(X_{(n)} \mid Y_{(n)})) < \epsilon$$

for any $n \geq n_0$ and any $d \in \mathbb{F}_q^\times$. Fix $\epsilon \in (0, 1/2)$. Then, there exists n_0 such that

$$Z_{\gamma d}(X_{(n)} \mid Y_{(n)})(1 - Z_d(X_{(n)} \mid Y_{(n)})) < \epsilon^2$$

for any $n \geq n_0$ and any $d \in \mathbb{F}_q^\times$, which in turn implies

$$Z_{\gamma d}(X_{(n)} \mid Y_{(n)}) < \epsilon \qquad \text{or} \qquad 1 - Z_d(X_{(n)} \mid Y_{(n)}) < \epsilon$$

for any $n \geq n_0$ and any $d \in \mathbb{F}_q^\times$. Assume $1 - Z_{d'}(X_{(n')} \mid Y_{(n')}) < \epsilon$ for fixed $n' \geq n_0$ and fixed $d' \in \mathbb{F}_q^\times$. Then, from

$$Z_{d'}(X_{(n')} \mid Y_{(n')})(1 - Z_{\gamma^{-1}d'}(X_{(n')} \mid Y_{(n')})) < \epsilon^2$$

one obtains $1 - Z_{\gamma^{-1}d'}(X_{(n')} \mid Y_{(n')})) < \epsilon^2/(1-\epsilon) < \epsilon$. By iterating this procedure, one proves that $1 - Z_{\gamma^i d'}(X_{(n')} \mid Y_{(n')})) < \epsilon$ holds for all $i \in \{0, \ldots, q-2\}$. In the same way, when $Z_{d'}(X_{(n')} \mid Y_{(n')}) < \epsilon$ is assumed for fixed $n' \geq n_0$ and fixed $d' \in \mathbb{F}_q^\times$, one can prove that $Z_{\gamma^i d'}(X_{(n')} \mid Y_{(n')})) < \epsilon$ holds for all $i \in \{0, \ldots, q-2\}$. This completes the proof of Lemma 15.

Appendix B
Bhattacharyya parameter and error probability

In this appendix, an unconditional version of Lemma 17 is proved. Lemma 17 itself is then proved straightforwardly by Jensen's inequality. For the proof of the unconditional version, one can regard $\mathcal{X}$ as any finite set whose size q is not necessarily a power of a prime. Let X be a random variable on $\mathcal{X}$. The optimum estimator for X minimizing the probability of error is given by $\hat{x} := \arg\max_x P_X(x)$, with the error probability

$$P_{\mathrm{e}}(X) := 1 - \max_{x \in \mathcal{X}} P_X(x).$$

The Bhattacharyya parameter is defined as

$$Z(X) := \frac{1}{q-1} \sum_{\substack{x \in \mathcal{X}, x' \in \mathcal{X}, \\ x' \neq x}} \sqrt{P_X(x) P_X(x')}.$$

The following lemma gives an upper bound of the error probability in terms of the Bhattacharyya parameter.

Lemma 31.

$$P_{\mathrm{e}}(X) \leq \min_{k=1,2,\ldots,q-1} \left\{ \frac{(q-1)Z(X) + k(k-1)}{k(k+1)} \right\}.$$

Proof: Noting that $P_X(\hat{x}) = 1 - P_{\mathrm{e}}(X)$ holds by the definition, one has

$$\sum_x \sqrt{P_X(x)} = \sqrt{1 - P_{\mathrm{e}}(X)} + \sum_{x \neq \hat{x}} \sqrt{P_X(x)}.$$

In order to prove the lemma, we first find the extremal distribution of X for which $Z(X)$ is minimized with $P_{\mathrm{e}}(X)$ fixed. As we will show, this amounts to minimizing the second term on the right-hand side with respect to $P_X(x)$ under the constraint that the error probability is $P_{\mathrm{e}}(X)$. We thus consider the following minimization problem for $\{p_i\}_{i=0,1,\ldots,q-2}$.

$$\begin{aligned} \text{minimize:} \quad & \sum_i \sqrt{p_i} \\ \text{subject to:} \quad & \sum_i p_i = P_{\mathrm{e}}(X) \\ & 0 \leq p_i \leq 1 - P_{\mathrm{e}}(X). \end{aligned}$$

Let $\{p_i^*\}_{i=0,1,\ldots,q-2}$ be the optimum solution of the minimization problem. Since $\sqrt{x}$ is a concave function, p_i^* is 0 or $1 - P_{\mathrm{e}}(X)$ except for at most one i [23]. Let $t-1$ be the number of p_i^*s which are equal to $1 - P_{\mathrm{e}}(X)$, then $t = \lfloor 1/(1 - P_{\mathrm{e}}(X)) \rfloor$ holds. The value of p_i^* which is not 0 or $1 - P_{\mathrm{e}}(X)$ is equal to $1 - t(1 - P_{\mathrm{e}}(X))$. Hence,

$$\sum_x \sqrt{P_X(x)} \geq t\sqrt{1 - P_{\mathrm{e}}(X)} + \sqrt{1 - t(1 - P_{\mathrm{e}}(X))}. \tag{18}$$

By squaring both sides of (18), one obtains the inequality

$$1 + (q-1)Z(X) \geq 1 + t(t-1)(1 - P_{\mathrm{e}}(X)) + 2t\sqrt{(1 - P_{\mathrm{e}}(X))(1 - t(1 - P_{\mathrm{e}}(X))}$$

which implies the minimum achievable value of the Bhattacharyya parameter for a given error probability. The right-hand side of the above inequality is further lower bounded by applying the inequality $1-P_{\mathrm{e}}(X) \geq 1-t(1-P_{\mathrm{e}}(X)) \Leftrightarrow t \geq 1/(1-P_{\mathrm{e}}(X))-1$ to the last term, yielding

$$\begin{aligned}(q-1)Z(X) &\geq t(t-1)(1-P_{\mathrm{e}}(X)) + 2t(1-t(1-P_{\mathrm{e}}(X)))\\ &= -(1-P_{\mathrm{e}}(X))t^2 + (1+P_{\mathrm{e}}(X))t. \end{aligned} \tag{19}$$

Since the quadratic function $-(1-P_{\mathrm{e}}(X))x^2 + (1+P_{\mathrm{e}}(X))x$ is concave and takes a maximum at $x = (1+P_{\mathrm{e}}(X))/(2(1-P_{\mathrm{e}}(X))$, which is the center of the unit interval $[P_{\mathrm{e}}(X)/(1-P_{\mathrm{e}}(X)), 1/(1-P_{\mathrm{e}}(X))]$ containing t, the inequality (19) still holds even if t is replaced by any integer $k = 1, 2, \dots, q-1$. ■

By replacing t by $1/(1-P_{\mathrm{e}}(X))$ in (19), one obtains a looser but smooth bound

$$P_{\mathrm{e}}(X) \leq \frac{(q-1)Z(X)}{(q-1)Z(X)+1}. \tag{20}$$

This bound is also obtained from the monotonicity of the Rényi entropy i.e., $H_{1/2}(X) \geq H_\infty(X)$. These upper bounds are plotted in Fig. 3 for $q = 5$.

The next lemma provides a lower bound of the error probability in terms of the Bhattacharyya parameter.

Lemma 32.

$$P_{\mathrm{e}}(X) \geq \frac{q-1}{q^2}\left(\sqrt{1+(q-1)Z(X)} - \sqrt{1-Z(X)}\right)^2. \tag{21}$$

Proof: We start with the same formula as that used as the starting point of the proof of Lemma 31.

$$\begin{aligned}\sum_x \sqrt{P_X(x)} &= \sqrt{1-P_{\mathrm{e}}(X)} + \sum_{x\neq\hat{x}} \sqrt{P_X(x)}\\ &= \sqrt{1-P_{\mathrm{e}}(X)} + (q-1)\sum_{x\neq\hat{x}} \frac{1}{q-1}\sqrt{P_X(x)}\\ &\leq \sqrt{1-P_{\mathrm{e}}(X)} + (q-1)\sqrt{\frac{1}{q-1}P_{\mathrm{e}}(X)}\\ &= \sqrt{1-P_{\mathrm{e}}(X)} + \sqrt{(q-1)P_{\mathrm{e}}(X)}. \end{aligned} \tag{22}$$

The above inequality is obtained from Jensen's inequality. This proof is the same as the proof of Fano's inequality for the Rényi entropy [24]. By squaring both sides of the above inequality, one has

$$\begin{aligned} & 1+(q-1)Z(X) \leq \left[\sqrt{1-P_{\mathrm{e}}(X)} + \sqrt{q-1}\sqrt{P_{\mathrm{e}}(X)}\right]^2\\ \iff\quad & Z(X) \leq \left((q-2)P_{\mathrm{e}}(X) + 2\sqrt{q-1}\sqrt{P_{\mathrm{e}}(X)(1-P_{\mathrm{e}}(X))}\right)/(q-1). \end{aligned}$$

The function

$$f(x) := \frac{(q-2)x + 2\sqrt{q-1}\sqrt{x(1-x)}}{q-1}$$

defined for $x \in [0, (q-1)/q]$ is continuous and strictly increasing since

$$\begin{aligned} f'(x) &= \frac{q-2}{q-1} + \frac{1-2x}{\sqrt{q-1}\sqrt{x(1-x)}}\\ f''(x) &= -\frac{1}{2\sqrt{q-1}(x(1-x))^{3/2}} < 0 \end{aligned}$$

and $f'((q-1)/q) = 0$. Hence, $f^{-1}(Z(X)) \leq P_{\mathrm{e}}(X)$ where the inverse function $f^{-1}(x)$ of $f(x)$ is

$$f^{-1}(x) = \frac{q-1}{q^2}\left(\sqrt{1+(q-1)x} - \sqrt{1-x}\right)^2.$$

■

Lemma 17 is obtained from Lemmas 31 and 32 by applying Jensen's inequality. The lower and upper bounds are plotted in Fig. 3 for $q = 5$. The bounds given in Lemma 17 are the tightest among those which are given in terms of the Bhattacharyya parameter only. Tight examples are shown below. The lower bound in Lemma 17 is tight for the q-ary symmetric channel, defined by $\mathcal{X} = \mathcal{Y} = \{0, \dots, q-1\}$ and

$$P_{Y|X}(y \mid x) = \begin{cases} 1-\epsilon, & \text{if } y = x\\ \epsilon/(q-1), & \text{if } y \neq x \end{cases}$$

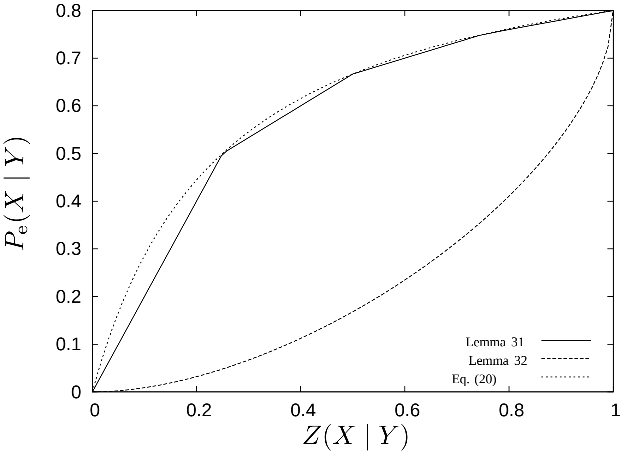


Fig. 3. The upper and lower bounds of error probability for $q = 5$.

for $\epsilon \in [0, (q-1)/q]$. In this case,

$$P_{\mathrm{e}}(X \mid Y) = \epsilon$$
$$Z(X \mid Y) = \frac{q-2}{q-1}\epsilon + 2\sqrt{\frac{\epsilon(1-\epsilon)}{q-1}}$$

which satisfies the lower bound with equality. The upper bound in Lemma 17 is tight for the following channel. Let $\mathcal{X} = \{0, \dots, q-1\}$. For fixed $k \in \{1, \dots, q-1\}$, let $\mathcal{Y} = \{a_{\mathcal{A}}\}_{\mathcal{A} \in A_k} \cup \{b_{\mathcal{B}}\}_{\mathcal{B} \in A_{k+1}}$ where $A_k := \{\mathcal{A} \subseteq \mathcal{X} \mid |\mathcal{A}| = k\}$.

$$P_{Y|X}(y \mid x) = \begin{cases} (1-\epsilon)/\binom{q-1}{k-1}, & \text{if } y = a_{\mathcal{A}} \text{ for } \mathcal{A} \in A_k \text{ and } x \in \mathcal{A} \\ \epsilon/\binom{q-1}{k}, & \text{if } y = b_{\mathcal{B}} \text{ for } \mathcal{B} \in A_{k+1} \text{ and } x \in \mathcal{B} \\ 0, & \text{otherwise} \end{cases}$$

for $\epsilon \in [0, 1]$. This satisfies the upper bound with equality since one has

$$P_{\mathrm{e}}(X \mid Y) = \frac{k^2 - 1 + \epsilon}{k(k+1)}$$
$$Z(X \mid Y) = \frac{k - 1 + \epsilon}{q-1}.$$

Appendix C
Proof of Lemma 18

Similarly to Appendix B, it is sufficient to prove an unconditional version of the inequalities in Lemma 18. Let $\mathcal{X}$ be a finite set of size q, and let X be a random variable on $\mathcal{X}$. Let

$$T(X) := \sum_{x \in \mathcal{X}} \left| P_X(x) - \frac{1}{q} \right|$$

be the total variation distance between P_X and the uniform distribution over $\mathcal{X}$.

Let $t := \lfloor 1/(1 - P_{\mathrm{e}}(X)) \rfloor$. The same argument as that of minimizing the concave function in Appendix B applies to minimizing $-T(X)$ given $P_{\mathrm{e}}(X)$, yielding the upper bound

$$\begin{aligned} T(X) &\le t\Big(1 - P_{\mathrm{e}}(X) - \frac{1}{q}\Big) + \left| 1 - t(1 - P_{\mathrm{e}}(X)) - \frac{1}{q} \right| + (q - t - 1)\frac{1}{q} \\ &= \frac{q-1}{q} + t\Big(1 - P_{\mathrm{e}}(X) - \frac{2}{q}\Big) + \left| \frac{q-1}{q} - t(1 - P_{\mathrm{e}}(X)) \right| =: f_T(P_{\mathrm{e}}(X)). \end{aligned}$$

We now derive the concave hull of $f_T(x)$ for obtaining the upper bound of $T(X \mid Y)$. Let k be a positive integer smaller than q. When x satisfies $(k-1)/k \le x < k/(k+1)$, one has $k \le 1/(1-x) < k+1$, so that the value of $t = \lfloor 1/(1-x) \rfloor$ is equal to the constant k. The function $f_T(x)$ is hence a convex function of x in the interval $(k-1)/k \le x < k/(k+1)$, and the linear interpolation of the values of $f_T(x)$ at the two endpoints $x = (k-1)/k$ and $x \uparrow k/(k+1)$ thus gives the concave hull of $f_T(x)$ for $(k-1)/k \le x < k/(k+1)$. One therefore obtains the inequality

$$f_T(x) \le (k+1)k\left[\big(k/(k+1)-x\big)f_T((k-1)/k) + \big(x-(k-1)/k\big)\lim_{x\uparrow k/(k+1)} f_T(x)\right]$$

for x satisfying $(k-1)/k \le x < k/(k+1)$. By substituting

$$f_T((k-1)/k) = \frac{2}{q}(q-k), \qquad\qquad \lim_{x\uparrow k/(k+1)} f_T(x) = \frac{2}{q}(q-k-1)$$

one obtains

$$\begin{aligned} f_T(x) &\le \frac{2}{q}(q-k-1) + \frac{2}{q}k\,\big[\big(k-(k+1)x\big)\big] \\ &= \frac{2(q-1)}{q} - \frac{2}{q}[-(1-x)k^2 + (1+x)k] \end{aligned}$$

and therefore

$$T(X) \le \frac{2(q-1)}{q} - \frac{2}{q}[-(1-P_\mathrm{e}(X))k^2 + (1+P_\mathrm{e}(X))k] \tag{23}$$

for $P_\mathrm{e}(X)$ satisfying $(k-1)/k \le P_\mathrm{e}(X) < k/(k+1)$. As shown in the proof of Lemma 31, the inequality (23) is correct for any $P_\mathrm{e}(X) \in [0,(q-1)/q]$. Note that by replacing k by $1/(1-P_\mathrm{e}(X))$, one obtains a looser but smooth upper bound

$$f_T(P_\mathrm{e}(X)) \le \frac{2}{1-P_\mathrm{e}(X)}\left(\frac{q-1}{q} - P_\mathrm{e}(X)\right).$$

The unconditional version of the other inequality in Lemma 18 is obtained by applying the triangle inequality, as

$$\begin{aligned} T(X) &= \left(1-P_\mathrm{e}(X)-\frac{1}{q}\right) + \sum_{x\ne\hat{x}}\left|P_X(x)-\frac{1}{q}\right| \\ &\ge \left(1-P_\mathrm{e}(X)-\frac{1}{q}\right) + \left|\sum_{x\ne\hat{x}}\left(P_X(x)-\frac{1}{q}\right)\right| = \left(1-P_\mathrm{e}(X)-\frac{1}{q}\right) + \frac{q-1}{q} - P_\mathrm{e}(X) \\ &= 2\left(\frac{q-1}{q} - P_\mathrm{e}(X)\right). \end{aligned}$$

Appendix D
Proof of Lemma 21

As before, it is again sufficient to prove an unconditional version of the inequalities in Lemma 21. The unconditional version $S(X)$ of $S(X \mid Y)$ is defined as

$$S(X) := \frac{1}{q-1}\sum_{w\in\mathbb{F}_q^\times}|P_X^*(w)| := \frac{1}{q-1}\sum_{w\in\mathbb{F}_q^\times}\left|\sum_{z\in\mathbb{F}_q}P_X(z)\chi(wz)\right|.$$

For the upper bound, one obtains

$$(q-1)S(X) = \sum_{w\in\mathbb{F}_q^\times}|P_X^*(w)| \le \sqrt{q-1}\sqrt{\sum_{w\in\mathbb{F}_q^\times}|P_X^*(w)|^2} = \sqrt{q(q-1)}\sqrt{\sum_{x\in\mathbb{F}_q}\left|P_X(x)-\frac{1}{q}\right|^2}.$$

Here, the inequality is obtained from the Cauchy-Schwarz inequality $\|p_0^{q-1}\|_1 \le \sqrt{q}\|p_0^{q-1}\|_2$ which holds for $p_0^{q-1} \in \mathbb{C}^q$. The last equality holds via Perseval's identity, i.e., since the Fourier transform is unitary up to the constant $\sqrt{q}$. Let $t := \lfloor 1/(1-P_\mathrm{e}(X))\rfloor$.

$$\begin{aligned} \sqrt{\sum_{x\in\mathbb{F}_q}\left|P_X(x)-\frac{1}{q}\right|^2} &\le \sqrt{t\left|1-P_\mathrm{e}(X)-\frac{1}{q}\right|^2 + \left|1-t(1-P_\mathrm{e}(X))-\frac{1}{q}\right|^2 + (q-t-1)\frac{1}{q^2}} \\ &= \sqrt{(1-P_\mathrm{e}(X))t\left((1-P_\mathrm{e}(X))t-P_\mathrm{e}(X)\right) - t(1-P_\mathrm{e}(X)) + \frac{q-1}{q}} \end{aligned} \tag{24}$$

Since (24) is piecewise convex with respect to $P_\mathrm{e}(X)$, its concave hull is

$$t(t+1)\left[(t/(t+1)-P_\mathrm{e}(X))\sqrt{\frac{q-1}{q}-\frac{t-1}{t}} + (P_\mathrm{e}(X)-(t-1)/t)\sqrt{\frac{q-1}{q}-\frac{t}{t+1}}\right]$$

for $P_{\mathrm{e}}(X) \in [0, (q-1)/q)$. Since this is piecewise linear and convex, t can be replaced by any $k = 1, \dots, q-1$. Note that the following smooth upper bound is obtained by replacing the first $(1 - P_{\mathrm{e}}(X))t$ in (24) by 1.

$$S(X) \le \sqrt{1 - \frac{q}{q-1} P_{\mathrm{e}}(X)}.$$

The unconditional version of the lower bound in Lemma 21 is obtained via the triangle inequality, as

$$\begin{aligned}
(q-1)S(X) + 1 = \sum_{w \in \mathbb{F}_q} |P_X^*(w)| &= \sum_{w \in \mathbb{F}_q} \left| \sum_{z \in \mathbb{F}_q} P_X(z) \chi(wz) \right| \\
&= \max_{a \in \mathbb{F}_q} \sum_{w \in \mathbb{F}_q} \left| \sum_{z \in \mathbb{F}_q} P_X(z) \chi(w(z-a)) \right| \\
&\ge \max_{a \in \mathbb{F}_q} \left| \sum_{z \in \mathbb{F}_q} P_X(z) \sum_{w \in \mathbb{F}_q} \chi(w(z-a)) \right| \\
&= q \max_{a \in \mathbb{F}_q} P_X(a) = q(1 - P_{\mathrm{e}}(X)).
\end{aligned}$$

Appendix E
Proof of Lemma 28

As in the argument for the binary case in [13, Chapter 5], MacWilliams identity is useful for the proof. Let $H := G^{-1}$ and $H_{\langle i \rangle} := [h_0, \dots, h_i]$ where h_i is the i-th column of H. Furthermore, we let the Fourier transform of the joint probability $P_{X,Y}$ be defined as $P_{X,Y}^*(w,y) := P_Y(y) P_{X|Y}^*(w \mid y)$. The generalized MacWilliams identity is obtained as follows.

$$\begin{aligned}
P_{X^{(i)},Y^{(i)}}(u_i, (u_0^{i-1}, y_0^{\ell-1})) &= \sum_{x_0^{\ell-1} \in \mathbb{F}_q^\ell} \mathbb{I}\{x_0^{\ell-1} H_{\langle i \rangle} = u_0^i\} \prod_{j=0}^{\ell-1} P_{X,Y}(x_j, y_j) \\
&= \sum_{x_0^{\ell-1} \in \mathbb{F}_q^\ell} \prod_{j=0}^{i} \left[\frac{1}{q} \sum_{w_j \in \mathbb{F}_q} \chi\Big(w_j \Big(\sum_{k=0}^{\ell-1} H_{kj} x_k - u_j \Big) \Big) \right] \prod_{j=0}^{\ell-1} \left[\frac{1}{q} \sum_{z_j \in \mathbb{F}_q} \chi(-z_j x_j) P_{X,Y}^*(z_j, y_j) \right] \\
&= \frac{1}{q^{\ell+i+1}} \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^i \in \mathbb{F}_q^{i+1}} \prod_{j=0}^{\ell-1} \left[\sum_{x_j \in \mathbb{F}_q} \chi\Big(x_j \Big(\sum_{k=0}^{i} H_{jk} w_k - z_j \Big) \Big) \right] \prod_{j=0}^{\ell-1} P_{X,Y}^*(z_j, y_j) \prod_{j=0}^{i} \chi(-w_j u_j) \\
&= \frac{1}{q^{i+1}} \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^i \in \mathbb{F}_q^{i+1}} \mathbb{I}\big\{ w_0^i H_{\langle i \rangle}^t = z_0^{\ell-1} \big\} \prod_{j=0}^{\ell-1} P_{X,Y}^*(z_j, y_j) \prod_{j=0}^{i} \chi(-w_j u_j).
\end{aligned}$$

Hence the Fourier transform $P_{X^{(i)},Y^{(i)}}^*$ of the joint probability $P_{X^{(i)},Y^{(i)}}$ is given by

$$P_{X^{(i)},Y^{(i)}}^*(w_i, (u_0^{i-1}, y_0^{\ell-1})) = \frac{1}{q^i} \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^{i-1} \in \mathbb{F}_q^i} \mathbb{I}\big\{ w_0^{i-1} H_{\langle i-1 \rangle}^t + w_i h_i^t = z_0^{\ell-1} \big\} \prod_{j=0}^{\ell-1} P_{X,Y}^*(z_j, y_j) \prod_{j=0}^{i-1} \chi(-w_j u_j).$$

Then, one can derive the first inequality in Lemma 28 as

$$\begin{aligned}
S_{\max}(X^{(i)}, Y^{(i)}) &= \max_{w_i \in \mathbb{F}_q^\times} \sum_{y_0^{\ell-1} \in \mathcal{Y}^\ell, u_0^{i-1} \in \mathbb{F}_q^i} |P_{X^{(i)},Y^{(i)}}^*(w_i, (u_0^{i-1}, y_0^{\ell-1}))| \\
&= \max_{w_i \in \mathbb{F}_q^\times} \sum_{y_0^{\ell-1} \in \mathcal{Y}^\ell, u_0^{i-1} \in \mathbb{F}_q^i} \left| \frac{1}{q^i} \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^{i-1} \in \mathbb{F}_q^i} \mathbb{I}\big\{ w_0^{i-1} H_{\langle i-1 \rangle}^t + w_i h_i^t = z_0^{\ell-1} \big\} \prod_{j=0}^{\ell-1} P_{X,Y}^*(z_j, y_j) \prod_{j=0}^{i-1} \chi(-w_j u_j) \right| \\
&\le \max_{w_i \in \mathbb{F}_q^\times} \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^{i-1} \in \mathbb{F}_q^i} \mathbb{I}\{ w_0^{i-1} H_{\langle i-1 \rangle}^t + w_i h_i^t = z_0^{\ell-1} \} \prod_{j=0}^{\ell-1} \sum_{y \in \mathcal{Y}} \big| P_{X,Y}^*(z_j, y) \big| \\
&\le q^i S_{\max}(X, Y)^{D_{\mathrm{s}}^{(i)}(G)}.
\end{aligned} \tag{25}$$

The last inequality in the above is obtained by observing that $z_0^{\ell-1}$ satisfying $w_0^{i-1} H_{\langle i-1 \rangle}^t + w_i h_i^t = z_0^{\ell-1}$ should contain at least $D_{\mathrm{s}}^{(i)}(G)$ nonzero elements, and that $\sum_{y \in \mathcal{Y}} |P_{X,Y}^*(0, y)| = 1$ holds.

As for the second inequality in Lemma 28, one has

$$\begin{aligned}
S_{\min}(X^{(i)}, Y^{(i)}) &= \min_{w_i \in \mathbb{F}_q^\times} \sum_{y_0^{\ell-1} \in \mathcal{Y}^\ell, u_0^{i-1} \in \mathbb{F}_q^i} |P^*_{X^{(i)},Y^{(i)}}(w_i, (u_0^{i-1}, y_0^{\ell-1}))| \\
&= \min_{w_i \in \mathbb{F}_q^\times} \sum_{y_0^{\ell-1} \in \mathcal{Y}^\ell, u_0^{i-1} \in \mathbb{F}_q^i} \left| \frac{1}{q^i} \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^{i-1} \in \mathbb{F}_q^i} \mathbb{I}\{w_0^{i-1} H^t_{\langle i-1 \rangle} + w_i h_i^t = z_0^{\ell-1}\} \prod_{j=0}^{\ell-1} P^*_{X,Y}(z_j, y_j) \prod_{j=0}^{i-1} \chi(-w_j u_j) \right| \\
&= \min_{w_i \in \mathbb{F}_q^\times} \max_{a_0^{i-1} \in \mathbb{F}_q^i} \sum_{y_0^{\ell-1} \in \mathcal{Y}^\ell, u_0^{i-1} \in \mathbb{F}_q^i} \left| \frac{1}{q^i} \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^{i-1} \in \mathbb{F}_q^i} \mathbb{I}\{w_0^{i-1} H^t_{\langle i-1 \rangle} + w_i h_i^t = z_0^{\ell-1}\} \right. \\
&\qquad \left. \cdot \prod_{j=0}^{\ell-1} P^*_{X,Y}(z_j, y_j) \prod_{j=0}^{i-1} \chi((a_j - w_j) u_j) \right| \\
&\geq \min_{w_i \in \mathbb{F}_q^\times} \max_{a_0^{i-1} \in \mathbb{F}_q^i} \sum_{y_0^{\ell-1} \in \mathcal{Y}^\ell} \left| \sum_{z_0^{\ell-1} \in \mathbb{F}_q^\ell, w_0^{i-1} \in \mathbb{F}_q^i} \mathbb{I}\{w_0^{i-1} H^t_{\langle i-1 \rangle} + w_i h_i^t = z_0^{\ell-1}\} \right. \\
&\qquad \left. \cdot \prod_{j=0}^{\ell-1} P^*_{X,Y}(z_j, y_j) \prod_{j=0}^{i-1} \left(\frac{1}{q} \sum_{u \in \mathbb{F}_q} \chi\big((a_j - w_j) u\big) \right) \right| \\
&= \min_{w_i \in \mathbb{F}_q^\times} \max_{a_0^{i-1} \in \mathbb{F}_q^i} \prod_{j=0}^{\ell-1} \sum_{y \in \mathcal{Y}} \left| P^*_{X,Y}((a_0^{i-1} H^t_{\langle i-1 \rangle} + w_i h_i^t)_j, y) \right| \\
&\geq \min_{w_i \in \mathbb{F}_q^\times} \max_{a_0^{i-1} \in \mathbb{F}_q^i} \prod_{j=0}^{\ell-1} S_{\min}(X, Y)^{\mathbb{I}\{(a_0^{i-1} H^t_{\langle i-1 \rangle} + w_i h_i^t)_j \neq 0\}} = S_{\min}(X, Y)^{D_{\mathrm{s}}^{(i)}(G)} \qquad (26)
\end{aligned}$$

where the last equality in the above is obtained by noting that the maximization with respect to a_0^{i-1} amounts to making the number of nonzero elements in $a_0^{i-1} H^t_{\langle i-1 \rangle} + w_i h_i^t$ to be as small as possible.

References

[1] R. Mori and T. Tanaka, "Channel polarization on q-ary discrete memoryless channels by arbitrary kernels," in *Proc. 2010 IEEE Int. Symp. Inf. Theory, Austin, TX.*, Jul. 13–18, 2010, pp. 894–898.

[2] ——, "Non-binary polar codes using Reed-Solomon codes and algebraic geometry codes," in *Proc. 2010 IEEE Information Theory Workshop, Dublin Ireland*, Aug. 30–Sep. 3, 2010.

[3] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[4] E. Şaşoğlu, E. Telatar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," 2009. [Online]. Available: http://arxiv.org/abs/0908.0302v1

[5] S. Korada, E. Sasoglu, and R. Urbanke, "Polar codes: Characterization of exponent, bounds, and constructions," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6253–6264, 2010.

[6] E. Arikan, "Source polarization," in *Proc. 2010 IEEE Int. Symp. Inf. Theory, Austin, TX.*, Jul. 13–18, 2010, pp. 899–903.

[7] H. Cronie and S. Korada, "Lossless source coding with polar codes," in *Proc. 2010 IEEE Int. Symp. Inf. Theory, Austin, TX.*, Jul. 13–18, 2010, pp. 904–908.

[8] N. Hussami, R. Urbanke, and S. Korada, "Performance of polar codes for channel and source coding," in *Proc. IEEE Int. Symp. Inf. Theory, Seoul, South Korea*, Jun. 28–Jul. 3 2009, pp. 1488–1492.

[9] E. Abbe and E. Telatar, "Polar codes for the m-user MAC," 2010. [Online]. Available: http://arxiv.org/abs/1002.0777

[10] S. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," *Information Theory, IEEE Transactions on*, vol. 56, no. 4, pp. 1751–1768, 2010.

[11] M. Karzand and E. Telatar, "Polar codes for q-ary source coding," in *Proc. 2010 IEEE Int. Symp. Inf. Theory, Austin, TX.* IEEE, Jun. 13–18, 2010, pp. 909–912.

[12] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Proc. IEEE Int. Symp. Inf. Theory, Seoul, South Korea*, Jun. 28–Jul. 3 2009, pp. 1493–1495.

[13] S. Korada, "Polar codes for channel and source coding," Ph.D. dissertation, Ecole Polytechnique Federale de Lausanne, 2009. [Online]. Available: http://library.epfl.ch/theses/?nr=4461

[14] R. Mori, "Properties and construction of polar codes," Master's thesis, Kyoto University, 2010. [Online]. Available: http://arxiv.org/abs/1002.3521

[15] S. Hassani, R. Mori, T. Tanaka, and R. Urbanke, "Rate-dependent analysis of the asymptotic behavior of channel polarization," *IEEE Trans. Inf. Theory*, 2012, to be published. [Online]. Available: http://arxiv.org/abs/1110.0194

[16] T. Tanaka and R. Mori, "Refined rate of channel polarization," in *Proc. 2010 IEEE Int. Symp. Inf. Theory, Austin, TX.*, Jun. 13–18, 2010, pp. 889–893.

[17] S. Hassani and R. Urbanke, "On the scaling of polar codes: I. the behavior of polarized channels," in *Proc. 2010 IEEE Int. Symp. Inf. Theory, Austin, TX.*, Jun. 13–18, 2010, pp. 874–888.

[18] J. Massey, D. Costello, and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Inf. Theory*, vol. 19, no. 1, pp. 101–110, Jan. 1973.

[19] K. Saints and C. Heegard, "On hyperbolic cascaded Reed-Solomon codes," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, vol. 673, pp. 291–303, May 1993.

[20] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North-Holland Amsterdam, 1977.

[21] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *Proc. 2009 IEEE Int. Symp. Inf. Theory, Seoul, South Korea*, Jun. 28–Jul. 3, 2009, pp. 1496–1500.

[22] R. Gallager, *Information Theory and Reliable Communication*. John Wiley & Sons, Inc. New York, NY, USA, 1968.

[23] M. Feder and N. Merhav, “Relations between entropy and error probability,” *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 259–266, Jan. 1994.

[24] M. Ben-Bassat and J. Raviv, “Renyi’s entropy and the probability of error,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 324–331, May 1978.